PCT/JP99/02510

17.06.99

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９８年１２月２８日

出願番号
Application Number: 平成１０年特許願第３７２１８７号

出願人
Applicant (s): 三菱マテリアル株式会社

１９９９年 ４月 ９日

特許庁長官
Commissioner,
Patent Office 伊佐山建志

出証番号 出証特平１１－３０２２７６８

【書類名】　特許願

【整理番号】　J76546A1

【提出日】　平成10年12月28日

【あて先】　特許庁長官　殿

【国際特許分類】　G09C　1/00

【発明の名称】　同報通信システム

【請求項の数】　27

【発明者】

【住所又は居所】　埼玉県大宮市北袋町１丁目２９７番地　三菱マテリアル株式会社　総合研究所内

【氏名】　大久保　達真

【発明者】

【住所又は居所】　埼玉県大宮市北袋町１丁目２９７番地　三菱マテリアル株式会社　総合研究所内

【氏名】　中根　一成

【発明者】

【住所又は居所】　埼玉県大宮市北袋町１丁目２９７番地　三菱マテリアル株式会社　総合研究所内

【氏名】　大木　直人

【発明者】

【住所又は居所】　埼玉県大宮市北袋町１丁目２９７番地　三菱マテリアル株式会社　総合研究所内

【氏名】　佐分利　徹

【特許出願人】

【識別番号】　000006264

【氏名又は名称】　三菱マテリアル株式会社

【代理人】

【識別番号】　100064908

【弁理士】

【氏名又は名称】　志賀　正武

【選任した代理人】

【識別番号】　100108578

【弁理士】

【氏名又は名称】　高橋　詔男

【選任した代理人】

【識別番号】　100089037

【弁理士】

【氏名又は名称】　渡邊　隆

【選任した代理人】

【識別番号】　100101465

【弁理士】

【氏名又は名称】　青山　正和

【選任した代理人】

【識別番号】　100094400

【弁理士】

【氏名又は名称】　鈴木　三義

【選任した代理人】

【識別番号】　100106493

【弁理士】

【氏名又は名称】　松冨　豊

【選任した代理人】

【識別番号】　100107836

【弁理士】

【氏名又は名称】　西　和哉

【選任した代理人】

【識別番号】　100108394

【弁理士】

【氏名又は名称】　今村　健一

【選任した代理人】

【識別番号】　100108453

【弁理士】

【氏名又は名称】　村山　靖彦

【選任した代理人】

【識別番号】　100100077

【弁理士】

【氏名又は名称】　大場　充

【手数料の表示】

【予納台帳番号】　008707

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9704954

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　同報通信システム

【特許請求の範囲】

【請求項１】　送信する情報を暗号化した暗号化情報を含む暗号情報を作成する暗号情報作成装置と、同報通信の被配信メンバーの公開鍵が含まれるメンバーリストを管理するメンバーリスト管理装置と、前記暗号化情報を復号化する暗号情報復号化装置と、前記暗号情報作成装置より送信された暗号情報を受信し、該暗号情報を前記メンバーリストをもとに１以上の前記暗号情報復号化装置に配信する情報中継装置と、からなる同報通信システムにおけるメンバーリスト管理装置であって、

同報通信を行う１以上のメンバーの公開鍵を含むメンバーリストを作成するリスト作成部と、

前記公開鍵を取得し保存する公開鍵管理部と

を備えることを特徴とするメンバーリスト管理装置。

【請求項２】　前記メンバーリスト管理装置は、

ネットワークを介して端末から、もしくは、装置に接続された記憶媒体から、前記メンバーリストを取得し保存するリスト取得保存部をさらに備えた

ことを特徴とする請求項１記載のメンバーリスト管理装置。

【請求項３】　前記メンバーリスト管理装置は、

前記メンバーリストをネットワークを介して、該ネットワークに接続されたデータベースまたは前記情報中継装置または前記メンバーリストに含まれるメンバーが利用する前記暗号情報作成装置ないし前記暗号情報復号化装置に送信するリスト送信部をさらに備えた

ことを特徴とする請求項１または請求項２に記載のメンバーリスト管理装置。

【請求項４】　前記メンバーリスト管理装置は、

同報通信のメンバーリストへの加入要求項目を設定する加入要求項目設定手段と、

加入要求者により入力・転送された加入要求が、前記加入要求項目を満たし、メンバーリストへの加入を許可するか否かをを判断する加入許可判断手段と、

からなる加入要求受付部をさらに備える

ことを特徴とする請求項１ないし請求項３のいずれかに記載のメンバーリスト管理装置。

【請求項５】　送信する情報を暗号化した暗号化情報を含む暗号情報を作成する暗号情報作成装置と、同報通信の被配信メンバーの公開鍵が含まれるメンバーリストを管理するメンバーリスト管理装置と、前記暗号化情報を復号化する暗号情報復号化装置と、前記暗号情報作成装置より送信された暗号情報を受信し、該暗号情報を前記メンバーリストをもとに１以上の前記暗号情報復号化装置に配信する情報中継装置と、からなる同報通信システムにおける暗号情報作成装置であって、

ネットワークを介して端末から、もしくは、装置に接続された記憶媒体から、前記メンバーリストを取得し保存するリスト取得保存部と、

同報通信文を取得し、該同報通信文を前記メンバーリストに含まれる公開鍵を用いて暗号化し暗号化情報とする暗号化部とを備えた

ことを特徴とする暗号情報作成装置。

【請求項６】　前記暗号化部は、

前記同報通信文を共通鍵暗号方式で暗号化した暗号文を作成し、

前記共通鍵暗号方式で用いた共通鍵を、前記メンバーリストに含まれる１以上の公開鍵を用いて公開鍵暗号方式で暗号化した１以上の暗号化共通鍵を作成し、

該暗号化共通鍵のうち、被配信メンバーに対応する暗号化共通鍵を選択するための鍵選択情報を作成し、

前記暗号情報として、前記暗号文、前記暗号化共通鍵、および前記鍵選択情報を出力する

ことを特徴とする請求項５に記載の暗号情報作成装置。

【請求項７】　前記暗号化部は、

同報通信文が複数の構成要素で構成されている場合、前記暗号化部は前記同報通信文を構成する個々の構成要素毎に暗号化し前記暗号情報を作成する

ことを特徴とする請求項５または請求項６に記載の暗号情報作成装置。

【請求項８】　前記暗号情報作成装置は、

同報通信文の送信先を検査し該送信先が前記情報中継装置でありかつ前記リスト取得保存部からメンバーリストを取得できた場合、該同報通信文を前記暗号化部へ送る宛先検査部をさらに備えた

ことを特徴とする請求項５ないし請求項７のいずれかに記載の暗号情報作成装置。

【請求項９】　前記暗号情報作成装置は、

同報通信文が主構成要素と１以上の従構成要素とからなる場合、主構成要素に対応する暗号情報に従構成要素に対応する暗号情報を参照可能とする参照情報を含め前記情報中継装置へ送信し、従構成要素に対応する暗号情報をネットワーク上の情報保管装置に送信する複数パーツ送信部をさらに備えた

ことを特徴とする請求項５ないし請求項８のいずれかに記載の暗号情報作成装置。

【請求項１０】　送信する情報を暗号化した暗号化情報を含む暗号情報を作成する暗号情報作成装置と、同報通信の被配信メンバーの公開鍵が含まれるメンバーリストを管理するメンバーリスト管理装置と、前記暗号化情報を復号化する暗号情報復号化装置と、前記暗号情報作成装置より送信された暗号情報を受信し、該暗号情報を前記メンバーリストをもとに１以上の前記暗号情報復号化装置に配信する情報中継装置と、からなる同報通信システムにおける暗号情報復号化装置であって、

前記情報中継装置から転送された暗号情報を取得する暗号情報取得部と、

前記暗号情報に含まれる暗号化情報を復号化する復号化部とを備えた

ことを特徴とする暗号情報復号化装置。

【請求項１１】　前記復号化部は、

前記暗号情報に含まれる鍵選択情報を参照し復号化に利用する暗号化共通鍵を選択する鍵選択部と、

公開鍵暗号方式を利用して前記選択した暗号化共通鍵を受信者の秘密鍵で復号化し、共通鍵を得る暗号化共通鍵復号化部と、

共通鍵暗号方式を利用して、前記共通鍵を用いて前記暗号情報に含まれる暗号化情報を復号化し、平文の同報通信文を得る暗号文復号化部とからなる

ことを特徴とする請求項１０に記載の暗号情報復号化装置。

【請求項１２】　前記暗号情報復号化装置は、

被配信メンバー本人が受信したことを通知する受信通知を前記情報中継装置に発信する受信通知発信部をさらに備える

ことを特徴とする請求項１０または請求項１１に記載の暗号情報復号化装置。

【請求項１３】　前記暗号情報復号化装置は、

同報通信文が主構成要素と１以上の従構成要素とからなる場合、従構成要素に対応する暗号情報を参照可能とする参照情報を含む主構成要素に対応する暗号情報を受信し、前記参照情報をもとに従構成要素に対応する暗号情報を受信する複数パーツ受信部をさらに備える

ことを特徴とする請求項１０ないし請求項１２のいずれかに記載の暗号情報復号化装置。

【請求項１４】　前記暗号情報復号化装置は、

前記暗号情報作成装置における暗号情報作成時に用いられたメンバーリストと、前記配信先リストを作成するために利用したメンバーリストの同一性の検証、

暗号情報の送信者がメンバーリストに含まれた者であるかかどうかの検証、

通信経路上で暗号情報が改竄されていないか検証する完全性の検証、

転送されてきた情報の中に悪意あるプログラムやデータ列が含まれているかどうかの検証、

転送されてきた暗号情報を参照して暗号情報作成装置で作成された複数のパーツからなる暗号情報のうち、一部が別の情報保管装置に転送されているかどうかの検証、

のいずれかもしくは組合わせによる前記検証を行なう同報通信安全性検証部をさらに備える

ことを特徴とする請求項１０ないし請求項１３のいずれかにに記載の暗号情報復号化装置。

【請求項１５】　前記暗号情報復号化装置は、

ネットワークを介してメンバーリストを既に保存している装置から、前記メンバーリストを取得し保存するリスト取得保存部をさらに備えた

ことを特徴とする請求項１０ないし請求項１４のいずれかに記載の暗号情報復号化装置。

【請求項１６】　送信する情報を暗号化した暗号化情報を含む暗号情報を作成する暗号情報作成装置と、同報通信の被配信メンバーの公開鍵が含まれるメンバーリストを管理するメンバーリスト管理装置と、前記暗号化情報を復号化する暗号情報復号化装置と、前記暗号情報作成装置より送信された暗号情報を受信し、該暗号情報を前記メンバーリストをもとに１以上の前記暗号情報復号化装置に配信する情報中継装置と、からなる同報通信システムにおける情報中継装置であって、

配信先リストを管理する配信先リスト管理部と、

転送されてきた暗号情報を複製する情報複製部と、

複製された暗号情報を各被配信メンバーに配信する送信部とを備える

ことを特徴とする情報中継装置。

【請求項１７】　前記配信先リスト管理部は、

必要なときに保存先からメンバーリストを取得可能であり、転送されたメンバーリストを保存するリスト取得保存部と、

チームマスターから転送されてきたメンバーリストに含まれるメンバーと同じメンバーに情報が配信されるように配信先リストを変更する

ことを特徴とする請求項１６に記載の情報中継装置。

【請求項１８】　前記情報中継装置は、

メンバーリストに添付された電子署名の正当性を確認する際に、該対応テーブルを参照して、自動的に正当なチームマスター本人の署名かどうかを判断させるリスト正当性確認部をさらに備える

ことを特徴とする請求項１６または請求項１７に記載の情報中継装置。

【請求項１９】　前記情報中継装置は、

転送されてきた情報の全部または一部に添付情報を添付する付加情報添付部をさらに備える

ことを特徴とする請求項１６ないし請求項１８のいずれかに記載の情報中継装置。

【請求項２０】　前記情報中継装置は、

前記暗号情報作成装置における暗号情報作成時に用いられたメンバーリストと、前記配信先リストを作成するために利用したメンバーリストの同一性の検証、

情報受信を拒否する受信側端末または利用者の識別情報が含まれる受信拒否情報を取得し、情報中継装置に転送されてきた情報の送信者または送信側端末が、前記受信拒否情報に含まれているか否かの検証、

暗号情報の送信者がメンバーリストに含まれた者であるかかどうかの検証、

通信経路上で暗号情報が改竄されていないか検証する完全性の検証、

転送されてきた情報の中に悪意あるプログラムやデータ列が含まれているかどうかの検証、

転送されてきた暗号情報を参照して暗号情報作成装置で作成された複数のパーツからなる暗号情報のうち、一部が別の情報保管装置に転送されているかどうかの検証、

のいずれかもしくは組合わせによる前記検証を行なう同報通信安全性検証部をさらに備える

ことを特徴とする請求項１６ないし請求項１９のいずれかに記載の情報中継装置。

【請求項２１】　前記情報中継装置は、

転送されてきた情報、または、情報の一部を保存しておく同報通信内容保存部をさらに備える

ことを特徴とする請求項１６ないし請求項２０のいずれかに記載の情報中継装置。

【請求項２２】　前記情報中継装置は、

同報通信サービスの開設受付の際に開設要求者が満たすべき開設要求項目を開設要求者の端末に提示させる開設要求項目提示手段と、

前記開設要求者が転送した開設受付要求が、前記開設要求項目を満たし、同報通信サービスの開設を許可するか否かをを判断する開設許可判断手段と、

前記開設許可判断手段により同報通信サービスの開設が決定されると、前記開設要求者をチームマスターとし、該チームマスターが指定したメンバーに情報を

配信する同報通信サービスを開設する同報通信開設手段と、

を含む同報通信自動開設部をさらに備える

ことを特徴とする請求項１６ないし請求項２１のいずれかに記載の情報中継装置。

【請求項２３】　請求項１ないし請求項４のいずれかに記載のメンバーリスト管理装置と、請求項５ないし請求項９のいずれかに記載の暗号情報作成装置と、請求項１０ないし請求項１５に記載の暗号情報復号化装置と、請求項１６ないし請求項２２のいずれかに記載の情報中継装置とからなる同報通信システム。

【請求項２４】　前記メンバーリスト管理装置におけるメンバーリスト管理プログラム記録した記録媒体であって、

同報通信を行う１以上のメンバーの公開鍵を含むメンバーリストを作成する手順と、

前記公開鍵を取得し保存する手順とを

をコンピュータに実行させるメンバーリスト管理プログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項２５】　前記暗号情報作成装置における暗号情報作成プログラム記録した記録媒体であって、

ネットワークを介して、メンバーリストを取得し保存する手順と、

同報通信文を取得し、該同報通信文を前記メンバーリストに含まれる公開鍵を用いて暗号化し暗号化情報とする手順と

をコンピュータに実行させる暗号情報作成プログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項２６】　前記暗号情報復号化装置における暗号情報復号化プログラム記録した記録媒体であって、

前記情報中継装置から転送された暗号情報を取得する手順と、

前記暗号情報に含まれる暗号化情報を復号化する手順と

をコンピュータに実行させる暗号情報復号化プログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項２７】　前記情報中継装置における情報中継プログラム記録した記

録媒体であって、

配信先リストを管理する手順と、

転送されてきた暗号情報を複製する手順と、

複製された暗号情報を各被配信メンバーに配信する手順と

をコンピュータに実行させる情報中継プログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、コンピュータネットワークを利用した同報通信の分野にあって、同報通信に利用される情報中継装置の管理者による不正を防止できる同報通信システムに関する。

【０００２】

【従来の技術】

近年、インターネット等のオープンなネットワークの普及によって、企業等の組織が持つＬＡＮ内だけではなく、インターネットに接続されたさまざまなメンバーと同報通信を行うことができるようになっている。同報通信とは、通信網上の多数の端末に同じ情報を一度に送信することを目的とした通信をいい、例えば電子メールシステムの場合には、メーリングリストを利用することによって同報通信を実現している。また、他の同報通信の例として、リアルタイムチャットなどもあげられる。

【０００３】

現在実現されている同報通信システムの一般的な例では、送信側端末は、同報通信を行うメッセージを受信者（被配信者）の集合（配信先リスト）を管理する情報中継装置に転送する。そして情報中継装置が配信するメッセージを受信者数分複製し、同報通信の各受信者に対して転送することにより同報通信を実現している。例えば、図１３に示す電子メールシステムでは、受信者の集合を示すメーリングリスト（Ｌｉｓｔ０１）を管理するメーリングリスト管理ホスト（Ｓｅｒｖｅｒ　Ａ）に対してメッセージを送り、このメーリングリスト管理ホストがメ

ーリングリストに挙げられている各受信者（Ｕｓｅｒ Ａ、Ｕｓｅｒ Ｂ、Ｕｓｅｒ Ｃ）に対してメッセージをコピーして送ることにより同報通信を実現している。

【０００４】

しかし、前述のようなオープンなネットワークアーキテクチャー上に構築された同報通信システムでは、各受信者に配信されるメッセージの覗き見や第三者への機密情報の漏洩等が常に問題となっていた。このような問題点を省みて、今日まで、ＥＤＩ（Electoronic Data Interchange）やＥＣ（Electoronic commerce）のようなネットワーク上における機密情報転送のニーズが高まり、同報通信システムにおいても、暗号技術を利用してセキュリティを高めた同報通信システムが研究・開発されている。

【０００５】

暗号技術を利用してセキュリティを高めた同報通信システムとして、特開平６－１５２５９２に開示されている同報通信システムがある。この発明では、暗号化に利用するデータ鍵と受信者を特定する宛先情報とシステムで共通のマスタ鍵とに基づいて暗号化鍵を生成し、この宛先情報と暗号化鍵を通信者間で送受信することにより、任意の一人または複数の通信相手とデータ鍵をを共有できる暗号通信方式を開示している。

【０００６】

しかし、このシステムを利用するにあたっては、セキュリティを確保するために、グループに属するメンバーを設定しておき、このメンバーに対しては、グループで暗号通信を行うために、ＩＣカード等の記憶媒体を配布しておく必要がある。しかし、現在利用されている同報通信（例えば、メーリングリスト）においては、グループに属するメンバーは脱退、加入等により動的に変化し、随時、配信先が変わるため、暗号同報通信においても、このような脱退、加入等に対応できることが望ましい。

【０００７】

次に、図１４に示す特開平７－２４５６０５に開示されている同報通信システムでは、メンバーの加入・脱退にも柔軟に対応できる同報通信システムを開示さ

れている。この同報通信システムにおける暗号化情報中継装置（Ｓｅｒｖｅｒ Ａ）は、通信回線で接続された複数の加入者間で情報の送受信を行うシステムにおいて、 発信加入者から送信され受信した暗号化情報の復号化（②）、または、受信加入者に送信する情報の暗号化（③）を行なう暗号計算部と、 暗号化情報を復号化するための共通秘密鍵と、各加入者（Ｕｓｅｒ Ａ、Ｕｓｅｒ Ｂ、Ｕｓｅｒ Ｃ）に対応した暗号化を行うための各加入者毎の個別公開鍵とを格納した鍵格納部とを有する暗号化情報中継装置をもつことを特徴としている。

【０００８】

しかし、この情報中継装置の管理者、もしくは、この管理者によって権限を委譲された者は、たとえ同報通信の加入者の中に含まれていない場合でも、暗号通信の通信内容を覗き見することができる。よって、悪意ある情報中継装置の管理者が存在する場合には、暗号通信で転送される機密情報が漏洩する危険性がある。例えば、企業間で行う同報通信での機密情報として企業の合併情報などが挙げられるが、これは、合併の影響を受ける情報中継装置の管理者に漏洩してはいけない情報である。

また、この情報中継装置は、必ず、暗号化情報の復号化処理、暗号化処理を行うことになる。しかし、暗号化処理・復号化処理は複雑で、大きな処理能力を必要とする。よって、同時に多数の暗号化情報が情報中継装置に到着した場合には、同報通信の遅延や、情報中継装置の処理能力を超えたために、動作不能に陥る危険性がある。

【０００９】

【発明が解決しようとする課題】

企業や組織、個人等が漏洩すると大きな損害を被るであろう機密情報を、限定された複数のメンバー間だけで同報通信を行うためには、以下のような課題を解決した同報通信システムを実現する必要がある。

（１）情報中継装置の管理者といえども、同報暗号通信の通信内容は、覗き見できない仕組みを実現し、本当に情報を共有する必要のあるメンバーにだけ同報通信内容が見られるようにする。

（２）同報通信を行う受信者の脱退や、加入に対して迅速に対応でき、同報通

信メンバーの動的な変更があっても、誤って同報通信してはいけないメンバーに情報を転送してしまうことを防止できるようにする。

（３）サーバ管理者が同報通信の配信メンバーを管理するのではなく、同報通信を行うメンバーの中で配信メンバーを管理し、さらにメンバーの管理者に集中する管理負担をできるだけ軽減する。

（４）機密情報を転送するため、多数の受信者それぞれが、確実に受信できる仕組みを確立する。

【００１０】

本発明は、上記の点に鑑みてなされたもので、 上記課題を解決する同報通信システムを構成するメンバーリスト管理装置、暗号情報作成装置、情報中継装置、暗号情報復号化装置、および、こららをコンピュータに実現させるプログラムを記録した記録媒体を提供するものである。

【００１１】

【課題を解決するための手段】

本発明のメンバーリスト管理装置は、送信する情報を暗号化した暗号化情報を含む暗号情報を作成する暗号情報作成装置と、同報通信の被配信メンバーの公開鍵が含まれるメンバーリストを管理するメンバーリスト管理装置と、前記暗号化情報を復号化する暗号情報復号化装置と、前記暗号情報作成装置より送信された暗号情報を受信し、該暗号情報を前記メンバーリストをもとに１以上の前記暗号情報復号化装置に配信する情報中継装置と、からなる同報通信システムにおけるメンバーリスト管理装置であって、同報通信を行う１以上のメンバーの公開鍵を含むメンバーリストを作成するリスト作成部と、前記公開鍵を取得し保存する公開鍵管理部とを備えることを特徴とする。

【００１２】

また、前記メンバーリスト管理装置は、ネットワークを介して端末から、もしくは、装置に接続された記憶媒体から、前記メンバーリストを取得し保存するリスト取得保存部をさらに備えたことを特徴とする。

【００１３】

また、前記メンバーリスト管理装置は、前記メンバーリストをネットワークを

介して、該ネットワークに接続されたデータベースまたは前記情報中継装置または前記メンバーリストに含まれるメンバーが利用する前記暗号情報作成装置ないし前記暗号情報復号化装置に送信するリスト送信部をさらに備えたことを特徴とする。

【００１４】

また、前記メンバーリスト管理装置は、同報通信のメンバーリストへの加入要求項目を設定する加入要求項目設定手段と、加入要求者により入力・転送された加入要求が、前記加入要求項目を満たし、メンバーリストへの加入を許可するか否かをを判断する加入許可判断手段と、からなる加入要求受付部をさらに備えることを特徴とする。

【００１５】

本発明の暗号情報作成装置は、送信する情報を暗号化した暗号化情報を含む暗号情報を作成する暗号情報作成装置と、同報通信の被配信メンバーの公開鍵が含まれるメンバーリストを管理するメンバーリスト管理装置と、前記暗号化情報を復号化する暗号情報復号化装置と、前記暗号情報作成装置より送信された暗号情報を受信し、該暗号情報を前記メンバーリストをもとに１以上の前記暗号情報復号化装置に配信する情報中継装置と、からなる同報通信システムにおける暗号情報作成装置であって、ネットワークを介して端末から、もしくは、装置に接続された記憶媒体から、前記メンバーリストを取得し保存するリスト取得保存部と、同報通信文を取得し、該同報通信文を前記メンバーリストに含まれる公開鍵を用いて暗号化し暗号化情報とする暗号化部とを備えたことを特徴とする。

【００１６】

また、前記暗号化部は、前記同報通信文を共通鍵暗号方式で暗号化した暗号文を作成し、前記共通鍵暗号方式で用いた共通鍵を、前記メンバーリストに含まれる１以上の公開鍵を用いて公開鍵暗号方式で暗号化した１以上の暗号化共通鍵を作成し、該暗号化共通鍵のうち、被配信メンバーに対応する暗号化共通鍵を選択するための鍵選択情報を作成し、前記暗号情報として、前記暗号文、前記暗号化共通鍵、および前記鍵選択情報を出力することを特徴とする。

【００１７】

また、前記暗号化部は、同報通信文が複数の構成要素で構成されている場合、前記暗号化部は前記同報通信文を構成する個々の構成要素毎に暗号化し前記暗号情報を作成することを特徴とする。

【００１８】

また、前記暗号情報作成装置は、同報通信文の送信先を検査し該送信先が前記情報中継装置でありかつ前記リスト取得保存部からメンバーリストを取得できた場合、該同報通信文を前記暗号化部へ送る宛先検査部をさらに備えたことを特徴とする。

【００１９】

また、前記暗号情報作成装置は、同報通信文が主構成要素と１以上の従構成要素とからなる場合、主構成要素に対応する暗号情報に従構成要素に対応する暗号情報を参照可能とする参照情報を含め前記情報中継装置へ送信し、従構成要素に対応する暗号情報をネットワーク上の情報保管装置に送信する複数パーツ送信部をさらに備えたことを特徴とする。

【００２０】

本発明の暗号情報復号化装置は、送信する情報を暗号化した暗号化情報を含む暗号情報を作成する暗号情報作成装置と、同報通信の被配信メンバーの公開鍵が含まれるメンバーリストを管理するメンバーリスト管理装置と、前記暗号化情報を復号化する暗号情報復号化装置と、前記暗号情報作成装置より送信された暗号情報を受信し、該暗号情報を前記メンバーリストをもとに１以上の前記暗号情報復号化装置に配信する情報中継装置と、からなる同報通信システムにおける暗号情報復号化装置であって、前記情報中継装置から転送された暗号情報を取得する暗号情報取得部と、前記暗号情報に含まれる暗号化情報を復号化する復号化部とを備えたことを特徴とする。

【００２１】

また、前記復号化部は、前記暗号情報に含まれる鍵選択情報を参照し復号化に利用する暗号化共通鍵を選択する鍵選択部と、公開鍵暗号方式を利用して前記選択した暗号化共通鍵を受信者の秘密鍵で復号化し、共通鍵を得る暗号化共通鍵復号化部と、共通鍵暗号方式を利用して、前記共通鍵を用いて前記暗号情報に含ま

れる暗号化情報を復号化し、平文の同報通信文を得る暗号文復号化部とからなることを特徴とする。

【００２２】

また、前記暗号情報復号化装置は、被配信メンバー本人が受信したことを通知する受信通知を前記情報中継装置に発信する受信通知発信部をさらに備えることを特徴とする。

【００２３】

また、前記暗号情報復号化装置は、同報通信文が主構成要素と１以上の従構成要素とからなる場合、従構成要素に対応する暗号情報を参照可能とする参照情報を含む主構成要素に対応する暗号情報を受信し、前記参照情報をもとに従構成要素に対応する暗号情報を受信する複数パーツ受信部をさらに備えることを特徴とする。

【００２４】

また、前記暗号情報復号化装置は、前記暗号情報作成装置における暗号情報作成時に用いられたメンバーリストと、前記配信先リストを作成するために利用したメンバーリストの同一性の検証、暗号情報の送信者がメンバーリストに含まれた者であるかかどうかの検証、通信経路上で暗号情報が改竄されていないか検証する完全性の検証、転送されてきた情報の中に悪意あるプログラムやデータ列が含まれているかどうかの検証、転送されてきた暗号情報を参照して暗号情報作成装置で作成された複数のパーツからなる暗号情報のうち、一部が別の情報保管装置に転送されているかどうかの検証、のいずれかもしくは組合わせによる前記検証を行なう同報通信安全性検証部をさらに備えることを特徴とする。

【００２５】

また、前記暗号情報復号化装置は、ネットワークを介してメンバーリストを既に保存している装置から、前記メンバーリストを取得し保存するリスト取得保存部をさらに備えたことを特徴とする。

【００２６】

本発明の情報中継装置は、送信する情報を暗号化した暗号化情報を含む暗号情報を作成する暗号情報作成装置と、同報通信の被配信メンバーの公開鍵が含まれ

るメンバーリストを管理するメンバーリスト管理装置と、前記暗号化情報を復号化する暗号情報復号化装置と、前記暗号情報作成装置より送信された暗号情報を受信し、該暗号情報を前記メンバーリストをもとに１以上の前記暗号情報復号化装置に配信する情報中継装置と、からなる同報通信システムにおける情報中継装置であって、配信先リストを管理する配信先リスト管理部と、転送されてきた暗号情報を複製する情報複製部と、複製された暗号情報を各被配信メンバーに配信する送信部とを備えることを特徴とする。

【００２７】

また、前記配信先リスト管理部は、必要なときに保存先からメンバーリストを取得可能であり、転送されたメンバーリストを保存するリスト取得保存部と、チームマスターから転送されてきたメンバーリストに含まれるメンバーと同じメンバーに情報が配信されるように配信先リストを変更することを特徴とする。

【００２８】

また、前記情報中継装置は、メンバーリストに添付された電子署名の正当性を確認する際に、該対応テーブルを参照して、自動的に正当なチームマスター本人の署名かどうかを判断させるリスト正当性確認部をさらに備えることを特徴とする。

【００２９】

また、前記情報中継装置は、転送されてきた情報の全部または一部に添付情報を添付し保存する付加情報添付部をさらに備えることを特徴とする。

【００３０】

また、前記情報中継装置は、前記暗号情報作成装置における暗号情報作成時に用いられたメンバーリストと、前記配信先リストを作成するために利用したメンバーリストの同一性の検証、情報受信を拒否する受信側端末または利用者の識別情報が含まれる受信拒否情報を取得し、情報中継装置に転送されてきた情報の送信者または送信側端末が、前記受信拒否情報に含まれているか否かの検証、暗号情報の送信者がメンバーリストに含まれた者であるかかどうかの検証、通信経路上で暗号情報が改竄されていないか検証する完全性の検証、転送されてきた情報の中に悪意あるプログラムやデータ列が含まれているかどうかの検証、転送され

てきた暗号情報を参照して暗号情報作成装置で作成された複数のパーツからなる暗号情報のうち、一部が別の情報保管装置に転送されているかどうかの検証、のいずれかもしくは組合わせによる前記検証を行なう同報通信安全性検証部をさらに備えることを特徴とする。

【００３１】

また、前記情報中継装置は、転送されてきた情報、または、情報の一部を保存しておく同報通信内容保存部をさらに備えることを特徴とする。

【００３２】

また、前記情報中継装置は、同報通信サービスの開設受付の際に開設要求者が満たすべき開設要求項目を開設要求者の端末に提示させる開設要求項目提示手段と、前記開設要求者が転送した開設受付要求が、前記開設要求項目を満たし、同報通信サービスの開設を許可するか否かをを判断する開設許可判断手段と、前記開設許可判断手段により同報通信サービスの開設が決定されると、前記開設要求者をチームマスターとし、該チームマスターが指定したメンバーに情報を配信する同報通信サービスを開設する同報通信開設手段と、を含む同報通信自動開設部をさらに備えることを特徴とする。

【００３３】

また、本発明は、請求項１ないし請求項４のいずれかに記載のメンバーリスト管理装置と、請求項５ないし請求項９のいずれかに記載の暗号情報作成装置と、請求項１０ないし請求項１５に記載の暗号情報復号化装置と、請求項１６ないし請求項２２のいずれかに記載の情報中継装置とからなる同報通信システムである。

【００３４】

また、本発明は、前記メンバーリスト管理装置におけるメンバーリスト管理プログラム記録した記録媒体であって、同報通信を行う１以上のメンバーの公開鍵を含むメンバーリストを作成する手順と、前記公開鍵を取得し保存する手順とををコンピュータに実行させるメンバーリスト管理プログラムを記録したコンピュータ読み取り可能な記録媒体である。

【００３５】

また、本発明は、前記暗号情報作成装置における暗号情報作成プログラム記録した記録媒体であって、ネットワークを介して、メンバーリストを取得し保存する手順と、同報通信文を取得し、該同報通信文を前記メンバーリストに含まれる公開鍵を用いて暗号化し暗号化情報とする手順とをコンピュータに実行させる暗号情報作成プログラムを記録したコンピュータ読み取り可能な記録媒体である。

【００３６】

また、本発明は、前記暗号情報復号化装置における暗号情報復号化プログラム記録した記録媒体であって、前記情報中継装置から転送された暗号情報を取得する手順と、前記暗号情報に含まれる暗号化情報を復号化する手順とをコンピュータに実行させる暗号情報復号化プログラムを記録したコンピュータ読み取り可能な記録媒体である。

【００３７】

また、本発明は、前記情報中継装置における情報中継プログラム記録した記録媒体であって、配信先リストを管理する手順と、転送されてきた暗号情報を複製する手順と、複製された暗号情報を各被配信メンバーに配信する手順とをコンピュータに実行させる情報中継プログラムを記録したコンピュータ読み取り可能な記録媒体である。

【００３８】

【発明の実施の形態】

まず、本発明の同報通信システムを構成するメンバーリスト管理装置、暗号情報作成装置、情報中継装置、暗号情報復号化装置の各実施の形態の説明にあたり、本発明の基本的技術思想および実施の形態の説明に用いる用語を説明する。図１に本発明の同報通信システムの概要を示している。なお、本発明の同報通信システムを構成する各装置の実施の形態は後ほど詳細に説明する。

【００３９】

従来の技術で説明したように、従来の同報通信では、情報中継装置（サーバ）に保存された被配信メンバー（受信者）の設定は、主にサーバ管理者、もしくは、サーバ管理者によって権限を委譲された者によって管理されていた。しかし、機密情報を同報通信する場合には、サーバ管理者が管理すべきでない同報通信を

行う可能性がある。

【００４０】

そこで本発明では、サーバ管理者ではなく、同報通信メンバー内のメンバーを管理する管理者（以降、チームマスターと称す）による被配信メンバーのリスト（以降、メンバーリストと称す）の管理を実現し、このメンバーリストが他者に改竄されない仕組みを提供する。そして、メンバーリストが安全かつ確実にメンバーリストに含まれるメンバーで共有され、メンバーが発信する同報通信の情報内容は暗号化され、情報が漏洩することなく、同報通信メンバーが安全かつ確実に機密情報を受信できるようにするものである。

【００４１】

まず、機密情報を安全かつ確実に同報通信をするには、通信相手となるメンバー本人を識別・認証する仕組みが必要となる。本発明では、本人を識別するための手法として、公開鍵暗号方式（例えば、ＲＳＡ（Rivest-Shamir-Adleman）方式や楕円暗号方式）における秘密鍵が、本人のみによって所有される仕組みを利用する。そのため、本発明のメンバーリストには、少なくとも、秘密鍵に対応する公開鍵が含まれる。また、メンバーリストが安全に管理されるようにするため、他者によって改竄されない仕組みを実現するため、チームマスターによる電子署名を添付する。

【００４２】

メンバーリストは、一般的には、チームマスターによって管理されるが、例えば、同報通信のメンバーの数が多く、一人の管理者で管理できない場合には、メンバーリストを複数のリストにわけ、チームマスターリストに含まれる複数の管理者（チームマスターと、チームマスターから権限を与えられたサブマスター）によって、管理される場合がある。図２に示すように、一般的なメンバーリストは、チーム名、チームマスターであるメンバーＸの名前もしくは識別子と、チームのメンバーであるメンバーＹ、…、メンバーＢの名前もしくは識別子と、このメンバーリストに対するチームマスターＸのデジタル署名（電子署名）からなる。また図３に、前述したようにメンバーリストが複数のリストからなる場合、特にメンバーリストをチーム１０１の管理者を登録したチームマスターリストと、

チーム１０１の同報通信メンバーを登録したメンバーリストに分割した場合の例を示している。この例のメンバーリストのデジタル署名は、チームマスターのＸのみならず、サブマスターのＹ、Ｚのデジタル署名であってもメンバーリストの正当性を確認できる。

【００４３】

この場合には、まず、メンバーリストの電子署名より、メンバーリストが改竄されていないかを検証し、署名者（この例では、メンバーＸ）を特定する。次に、チームマスターリストの電子署名より、チームマスターリストが改竄されていないかを検証し、さらにチームマスターの署名者が間違いなくこのチームのチームマスターかどうかを確認する。最後にこのメンバーリストの署名者が、チームマスターリストにチームの管理者として登録されているかを検証する。図３の例では、メンバーＸは、チームマスターとして登録されているので、正当な署名者であると判断できる。また、メンバーリストにメンバーＹによる署名が添付されていた場合でも、メンバーＹは、メンバーＸより管理権限を委譲された正当な署名者（ここでは、サブマスターとする－図３中では、「サブ」と記載している）として判断できるため、正当性を検証できる。

【００４４】

また、メンバーリストには、一人のメンバーに対して、複数の公開鍵を登録する方式としてもよい。例えば、暗号化・復号化処理に利用する公開鍵と秘密鍵のペアと、電子署名作成・検証処理に利用する公開鍵と秘密鍵のペアを、それぞれ異なる鍵ペアを利用する場合には、各メンバーに対して２つの公開鍵が登録されていることになる。

【００４５】

また、メンバーリストには公開鍵を登録するが、この公開鍵として認証局より発行されたデジタル証明書（例えば、Ｘ．５０９フォーマットに従ったデジタル証明書であり、以降、証明書と称す）を利用することができる。また、メンバーリストに、公開鍵本体を一意に識別するための情報を登録する方式を利用してもよい。この場合は、公開鍵本体は、各メンバーがすでに保有している場合には、公開鍵を識別する情報（例えば、信頼できる認証局より発行された証明書に含ま

れる公開鍵を利用している場合には、その証明書に与えられたシリアルＮｏ．や認証局名、証明書をハッシュ関数で圧縮したメッセージダイジェスト）をメンバーリストに含めておけば、各メンバーは、メンバーリストを受け取った後、暗号化に利用する実際の公開鍵本体を選択もしくは、取得することができる。例えば、メンバーリストに認証局名とシリアルＮｏ．が含まれていた場合には、まず、端末に接続された記憶媒体に保存された複数の証明書から、この認証局名とシリアルＮｏ．をもつ証明書を検索し、記憶媒体に存在しなかった場合には、この認証局名の認証局に問い合せこのシリアルＮｏ．の証明書を取得することもできる。

【００４６】

以下に、本発明の同報通信システムを構成するメンバーリスト管理装置、暗号情報作成装置、情報中継装置、暗号情報復号化装置の各実施の形態を図面を参照し順に説明する。

【００４７】

図４は、本発明のメンバーリスト管理装置の第１から第４の実施の形態を包含し表している。

まず、メンバーリスト管理装置１の第１の実施の形態を説明する。本実施の形態は、メンバーリストを管理するために、同報通信を行う１以上のメンバーの公開鍵を含むメンバーリストを作成するリスト作成部１ａと、メンバーリストに含める公開鍵を取得し保存する公開鍵管理部１ｂとから構成される。

【００４８】

はじめにチームマスターが、メンバーリスト管理装置１を利用してメンバーリストを作成するための所定の項目（メンバーの情報等）を入力する。データの入力後、図５に示すようにリスト作成部１ａは、メンバーとして登録するメンバーの公開鍵を選択する（ステップＳ１）。例えば、図２に示すメンバーリストを作成する場合、メンバーＸ、Ｙ、…、Ｂの公開鍵が選択される。そして、ハッシュ関数（例えば、ＭＤ５やＳＨＡ－１等）を利用してメンバーリストのメッセージダイジェストを作成する（ステップＳ２）。そして、作成したメッセージダイジェストをチームマスターの秘密鍵で暗号化して（例えば、ＲＳＡやＤＳＡを利用

して）作成した電子署名をメンバーリストに添付（ステップＳ３；図２の例では、Ｘのデジタル署名を添付）する仕組みとする。この仕組みにより、後述の情報中継装置以外の端末（図示せず）をメンバーリスト管理装置１として利用しても、メンバーリストを改竄される心配はない。現実に改竄された場合には、メンバーリストの正当性を検証することにより改竄が発覚するため、改竄されたメンバーリストの使用を中止することが可能である。

【００４９】

次に、メンバーリスト管理装置１の第２の実施の形態として、第１の実施の形態のメンバーリスト管理装置１に、さらにリスト取得保存部１ｃを備えた構成をとる。

リスト取得保存部１ｃは、メンバーリスト管理装置１に接続された記憶媒体に対するメンバーリストの取得保存を行なうように動作するだけでなく、メンバーリスト管理装置１が接続されたネットワークに配置された端末（例えば、サーバ）やデータベース（図示せず）を利用して、これらの端末やデータベースにアクセスし、メンバーリストを取得または保存するように動作する。

この構成をとるのは、あるチームマスターがメンバーリストを管理している間に、チームマスターの端末に障害が発生した場合や、誤ってメンバーリストが消去される危険性があるため、チームマスターの端末でなく、ネットワーク上の安全な端末（例えば、サーバ）またはデータベースにメンバーリストを保存しておくと、より安全であるからである。

【００５０】

また、同報通信の管理負担が一人の管理者に集中すること軽減し、操作ミス等を未然に防止するため、複数の管理者（チームマスターと複数のサブマスター）でメンバーリストを管理する形態もある。この場合、各管理者が異なるバージョンのメンバーリストを利用することが無いように、各管理者がアクセスできるネットワーク上の端末またはデータベースに、メンバーリストを保存する方がより完全性を保った同報通信を実現できる。

【００５１】

本発明の同報通信システムは、メンバーリストに含まれる公開鍵によって暗号

化を行うことによって、同報通信メンバー外への情報の漏洩を防ぐ（例えば、サーバ管理者への情報の漏洩を防ぐ）仕組みを実現している。よって、メンバーリスト管理装置１では、メンバーリストが正当性をもって管理されているかを検証する必要がある。ここでいう正当性の検証とは、１）メンバーリストが、権利のない者に改竄されていない状態を維持している、かつ、２）メンバーリストを作成した者が同報通信を行うチームの正式なチームマスターである、状態を確認することである。

【００５２】

１）については、例えば、メンバーリストに添付された電子署名（図２の例では、Ｘのデジタル署名）を復号化してメンバーリストのメッセージダイジェストを取得し、さらに、メンバーリスト（図２の例では、チーム１０１、メンバーＸ、メンバーＹ…メンバーＢを内容としてもつリスト）をメンバーリスト作成時に用いられたものと同じハッシュ関数で圧縮して得たメッセージダイジェストを取得し、双方を比較することにより検証できる。また、２）については、例えば、メンバーリストへの署名者の名前（例えば、Ｘ．５０９の証明書フォーマットに従う証明書に記載された名前）をメンバーリスト利用者が確認できるように画面に表示し、確認してもらうことにより検証できる。

【００５３】

リスト取得保存部１ｃは、メンバーリストを識別する情報とメンバーリストを管理するチームマスターを対応づける対応テーブルを作成し保存する機能と、メンバーリストに添付された電子署名の正当性を確認する際に、この対応テーブルを参照して、電子署名が正当なチームマスター本人の署名であるかどうかを判断させる機能をさらに備えることでメンバーリストの正当性を検証できる。

また、対応テーブルを作成するにあたっては、例えば、初めて取得するメンバーリストの場合には、メンバーリスト利用者がチームマスターを確認できるように画面に表示し、確認してもらうことにより検証する。ここで肯定指示（メンバーリストの署名者としてこのチームマスターを認める場合）が出た場合には、メンバーリストを識別する情報（図２の例では、チーム名の「チーム１０１」）とメンバーリストを管理するチームマスター（図２の例では、チームマスターであ

る「メンバーＸ」）を、テーブルに追加する追加機能をさらに備えることで、２回目以降は、自動的に正当性確認が行われるようになる。

ここで説明した、メンバーリストの正当性を検証する機能は、後述の暗号情報作成装置、暗号情報復号化装置、情報中継装置のそれぞれにおいても備えられ、メンバーリストの取得時もしくはメンバーリストを利用する際に機能する。

【００５４】

次に、メンバーリスト管理装置１の第３の実施の形態として、第１もしくは第２の実施の形態のメンバーリスト管理装置１に、リスト送信部１ｄをさらに備えた構成をとる。

リスト送信部１ｄは、メンバーリストに含まれるメンバーが利用する端末にメンバーリストを送信するように動作する。

この構成をとることにより、最新のメンバーリストをメンバーリストのメンバー間で迅速かつ正確に共有することができる。

【００５５】

また、チームマスターはさらに、後述する情報中継装置が情報を再配信する際に参照する配信先リストを変更する必要がある。この配信先リストを変更する仕組みは、情報中継装置の種類や仕組みによって異なってくる。例えば、音声チャットの同報通信システムとメールの同報通信システムでは、装置の構造やプロトコルが異なる。本実施の形態のメンバーリスト管理装置１では、利用するシステムによって操作方法が異なることの無いように、メンバーリストに含まれるメンバーと配信先リストに含まれるメンバーが同一になるように、メンバーリスト管理装置１に配信先リストを変更する機能をさらに付加してもよい。この配信先リストを変更する機能として、もっとも簡単な実施形態としては、本実施の形態のリスト送信部１ｄからメンバーリストを情報中継装置に転送し、情報中継装置ではこのメンバーリストを配信リストとして用いる方式があげられる。

【００５６】

本発明のメンバーリスト管理装置の第４の実施の形態として、第１ないし第３のいずれかの実施の形態のメンバーリスト管理装置１に、加入要求受付部１ｅをさらに備えた構成をとる。

【００５７】

加入要求受付部１ｅは、同報通信のメンバーリストへの加入要求を受け付けるために、同報通信のチームマスターが、特定同報通信の配信リストへの加入要求項目を設定する加入要求項目設定機能と、加入要求を受付ける際に加入要求者が満たすべき項目を提示するための加入要求項目提示機能と、加入要求者が転送してきた加入要求が、加入要求項目を満たし、加入を許可するか否かをを判断する加入許可判断機能を備える。

また、本実施の形態の加入要求受付部１ｅは、加入要求が正確な要求であるかどうかを検証する際に、ネットワーク上に配置されたデータベースやサーバ等に、問い合わせて検証を行なう。例えば、加入項目にクレジットカードＮｏ．が記載されていた場合には、このクレジットカードＮｏ．の有効性をクレジットカード会社が運用する端末にアクセスして検証したり、証明書が含まれていた場合には、認証局が運用する証明書データベースにアクセスして検証することができる。

【００５８】

上述の加入要求受付部１ｅの機能により、同報通信への受信者の自動加入を実現することができる。現在実現されている同報通信への受信者の自動加入の一例として、例えば、メーリングリストへの加入プロセスを自動化し、ユーザがＷＷＷページで登録するとメーリングリストに自動的に加入できるシステムがある。しかし、現在のメーリングリストは、情報中継装置の管理者の権限で起動されるプロセスを自動化したものであり、現在の自動化プロセスでは、情報中継装置の管理者が、配信メンバーを自由に設定できる仕組みを提供しているにすぎない。本実施の形態の加入要求受付部１ｅは、悪意ある情報中継装置の管理者などによる不正を防止し、より安全性の高い自動加入の仕組みを提供するためのものである。

【００５９】

ここで、メンバーリストに含まれる公開鍵や、秘密鍵は、間違いなく本人のものかどうか、また、使用期限などを設定していた場合に期限切れでないか、また、すでに秘密鍵が漏洩していないかを検証してから利用する方が望ましい。した

がって、メンバーリスト管理装置１の各実施の形態では、ネットワーク上に配置されたデータベース（例えば、認証局やサービス企業が提供する公開鍵の有効性や信頼性をあらわす状態を登録したディレクトリデータベースなど）に、同報通信と同じまたは、異なるプロトコル（例えば、同報通信でＳＭＴＰ（Simple Mail Transfer Protocol）を利用する場合には、ＬＤＡＰ（Lightweight Directory Access Protocol）、ＯＣＳＰ（Online Certificate Status Protocol）など）を利用して問い合わせを行ったり、認証局より配布される証明書廃棄リスト（ＣＲＬ（Certificate Revocation List））を利用して、公開鍵や電子署名に利用される秘密鍵の有効性を検証する形態としてもよい。

ここで説明した、公開鍵や電子署名に利用される秘密鍵の有効性を検証する機能は、後述の暗号情報作成装置、情報中継装置、暗号情報復号化装置のそれぞれにおいてもこの機能を備えることにより、電子署名の確認やメンバーリストの管理の際に有効となる。

以上、本発明のメンバーリスト管理装置の各実施の形態を説明した。

【００６０】

次に、本発明の暗号情報作成装置の実施の形態を説明する。図６は、本発明の暗号情報作成装置の第１から第３の実施の形態を包含し表している。

【００６１】

本発明の暗号情報作成装置の第１の実施の形態は、ネットワークを介してメンバーリストを取得し保存するリスト取得保存部２ａと、暗号情報を作成する暗号化部２ｂとから構成される。

【００６２】

リスト取得保存部２ａは、ネットワーク上に配置されたリソースデータベースに保存されたメンバーリストを、同報通信と同じ、または、異なるプロトコル（例えば、同報通信でＳＭＴＰを利用する場合には、ＨＴＴＰなど）を利用して取得する。または、転送されてきたメンバーリストを記憶装置（図示せず）に保存し、必要なときに保存先からメンバーリストを読み込むことにより取得する。

【００６３】

また、暗号情報作成装置２がすでにメンバーリストを保存している場合には、

リスト取得保存部２ａは、メンバーリストが最新バージョンか確認するように動作する。例えば、メンバーリストの最新バージョンに関する情報が保存されたネットワーク上に配置されたデータベースに、同報通信と同じまたは、異なるプロトコル（例えば、同報通信でＳＭＴＰを利用す場合には、ＬＤＡＰ、ＯＣＳＰなど）を利用して、最新のメンバーリストのバージョンを問い合わせ確認する。また、リスト取得保存部２ａは、前述のメンバーリスト管理装置１の実施の形態で説明したメンバーリストの正当性を検証する機能を備え、メンバーリストの取得時にメンバーリストの正当性を検証する。

なお、記憶部（図示せず）は、ＥＥＰＲＯＭ、ハードディスク、光磁気ディスク等の不揮発性の記憶装置により構成されている。

【００６４】

次に、暗号化部２ｂは、図７に示すようにまず同報通信文（平文）とリスト取得保存部２ａにより取得されたメンバーリストを取得し、同報通信文を共通鍵暗号方式（例えば、ＤＥＳ等の暗号化と復号化で同じ鍵を利用する暗号方式）で暗号化し暗号文を作成する。

そして暗号文作成に用いた共通鍵を、メンバーリストに含まれる各メンバー公開鍵を用いて、公開鍵暗号方式（例えば、ＲＳＡ方式）により暗号化した暗号化共通鍵を作成する。このときメンバーが３名ならば、３つの暗号化共通鍵が作成されることになる。

さらに複数の暗号化共通鍵のうち、被配信メンバーに対応する暗号化共通鍵を選択するための鍵選択情報を作成する。この鍵選択情報として、例えば、メンバー名と暗号化共通鍵を対応させるテーブルを用いてもよい。

また、同報通信文をハッシュ関数で圧縮し、送信者の秘密鍵で暗号化した電子署名を付加する。この電子署名により改竄防止、送信者の確認ができるようになる。

そして暗号情報として、暗号文、暗号化共通鍵、鍵選択情報、および電子署名を出力するように動作する。

なお、同報通信システムにおいて、この暗号情報作成装置２は送信側端末で利用されるものである。

【００６５】

次に、暗号情報作成装置２の第２の実施の形態は、図６に示すように第１の実施の形態に宛先検査部２ｃをさらに備える構成をとる。

宛先検査部２ｃは同報通信文の送信先を検査し、情報中継装置が送信先となっていて、かつ、同報通信に利用するメンバーリストが取得できる場合にのみ、同報通信文を暗号化部２ｂへ渡すように動作する。

この宛先検査部２ｃを設けることで、暗号情報作成装置２は暗号化処理だけを行うように実施でき、したがって同報通信文自体の作成は、汎用的なメッセージ作成装置（ワードプロセッサーや、メーラー、チャットクライアント等）を利用できる。

【００６６】

例えば、暗号情報作成装置２をメーラーのプラグイン・ソフトとして実現した場合、メールの文章および添付ファイルの作成までは、既存のメーラーの機能を利用できる。暗号情報作成装置２としてのプラグイン・ソフトは、メール送信前に宛先を検査し、メーリングリスト・サーバのアドレスが宛先となっていた場合には、このアドレスに対応するメンバーリストを取得し、メンバーリストに含まれる公開鍵を利用して上述の暗号化を行い暗号情報を作成する。この暗号情報は、既存のメールが利用する通信機能（例えば、プロトコルとしてＳＭＴＰを利用した通信機能）を利用して、メーリングリスト・サーバへと送信される。

なお、本実施の形態の暗号情報作成装置２に、同報通信文を作成する専用の同報通信情報作成部（図示せず）をさらに備えてもよい。

【００６７】

次に、暗号情報作成装置２の第３の実施の形態は、図６に示すように第１または第２の実施の形態に複数パーツ送信部２ｄをさらに備える構成をとる。

本実施の形態では、暗号化部２ｂは、同報通信文が複数のパーツで構成されている場合には、個々のパーツごとに前述の暗号化処理を行い暗号情報を作成する。そして、複数パーツ送信部２ｄは、図８に示すように同報通信文が複数のパーツで構成されている場合、情報中継装置の受信能力に応じてパーツのうちのいくつかを情報中継装置から参照できる情報保管装置５に送信するように動作する。

この際、各パーツの送信に最適なプロトコルを用いることができる。例えば、音声チャットには、リアルタイム通信プロトコル、ファイルの転送には、ファイル転送プロトコルを利用する。

【００６８】

なお、複数パーツ送信部２ｄは、ネットワーク上に配置されたリソースデータベースまたは、情報中継装置４に問い合わせることで、情報中継装置４から参照でき同報通信文の一部を転送しても良い情報保管装置５を知る。また、別の方法として、メンバーリストに情報保管装置５のアドレスを含め利用してもよい。

また、複数パーツを別々の装置に送信する場合には、受信者は、もとの情報が全部揃ったかどうかを検証する必要がある場合がある。その場合には、それぞれの暗号化処理を行なった際に、もとの全平文パーツもしくは、全暗号文パーツもしくは、各平文パーツのメッセージダイジェストの集合もしくは、各暗号文パーツのメッセージダイジェストの集合のうち一つもしくは、いくつかを組み合わせた情報に対してハッシュ関数を利用して作成したメッセージダイジェストもしくは、このメッセージダイジェストに電子署名したものを添付することにより、各情報をまったく異なる装置に転送した場合でも、同報通信文全体の完全性を検証することができる。

【００６９】

本実施の形態では、各パーツの複数のプロトコルにまたがる通信となっても、情報の暗号化処理およびメンバーリストは同一のものを利用し、確実にチームマスターが設定したメンバー間での同報通信が行え、各パーツの同報通信の安全性、確実性のレベルを等しくすることができる。

【００７０】

本実施の形態は、同報暗号通信システムにおいて、異なるフォーマットのメッセージを同時に同報通信する場合に有効である。例えば、音声チャット同報通信システムを利用して、複数の企業にまたがるメンバーが商談を行いながら、同時に、契約書ファイルを転送する場合や、メーリングリスト同報通信システムを利用して、メンバーに対して暗号メールを送信するとともに、メールシステムの許容量を超えるような大きなファイル（例えば、５Ｍｂｙｔｅの画像ファイル）を

転送する場合がある。例えば、音声チャットの場合には、契約書ファイルを転送しようとした時点で、音声チャットの音声が途切れてしまい同報通信が不通となるようでは、重要な機密情報を取り扱っている場合には、聞き落とし等が発生する危険性がある。

【００７１】

また、メーリングリスト同報通信装置では、それぞれの受信側メールシステムの設定によって許容量（例えば、メンバーＡのシステムでは、３Ｍｂｙｔｅ、メンバーＢのメールシステムでは、１Ｍｂｙｔｅ）が異なる上、特定メンバー用に確保されたメール受信用のバッファにどの程度空き容量あるかによって、受信能力が異なるため、送信者は、確実に送信できるか想定しがたい。本実施の形態は、これらの環境においても有効に機能するものである。

【００７２】

また、暗号化時に利用するメンバーリストに含まれる公開鍵は、暗号化に利用する前に有効性を検証する方がより、セキュリティの安全性が向上する。例えば、チームマスターがメンバーリストを作成した時点では、すべての公開鍵が有効であっても、一定期間後同じ鍵を使おうとしても、使用期限を迎えた鍵が存在したり、秘密鍵が漏洩している可能性がある。暗号情報作成装置２の各実施の形態では、メンバーリスト管理装置１の公開鍵や電子署名に利用される秘密鍵の有効性を検証する機能と同様の鍵有効性検証機能を備えることによりさらに安全性が向上する。

以上、本発明の暗号情報作成装置の各実施の形態を説明した。

【００７３】

次に、本発明の暗号情報復号化装置の実施の形態を説明する。図９は、本発明の暗号情報復号化装置の第１から第５の実施の形態を包含し表している。

【００７４】

暗号情報復号化装置３の第１の実施の形態は、後述する情報中継装置から転送されてきた暗号情報を取得する暗号情報取得部３ａと、暗号情報を復号化する復号化部３ｂとから構成される。

復号化部３ｂは、図７に示すようにまず暗号情報に含まれる鍵選択情報を参照

しメンバー数に相当する複数の暗号化共通鍵の中から復号化に使用する暗号化共通鍵を選択する。そして暗号化共通鍵を公開鍵暗号方式を利用して受信者の秘密鍵を用いて復号化し共通鍵を得る。そして、共通鍵暗号方式を利用して、共通鍵を使用し暗号情報に含まれる暗号文を復号化し、平文の同報通信文を得る。そして、電子署名を送信者の公開鍵で復号化たメッセージダイジェストＭＤと、暗号文を復号化した同報通信文（平文）をハッシュ関数で圧縮したメッセージダイジェストＭＤ’を比較・検証し、改竄や送信者の確認を行なう。

【００７５】

次に、暗号情報復号化装置３の第２の実施の形態として、図９に示すように第１の実施の形態の暗号情報復号化装置に、さらに受信者本人が受信したことを確認するための受信通知を情報中継装置に発信する受信通知発信部３ｃを備える構成をとる。受信通知発信部３ｃは、例えば、受信した通信内容のメッセージダイジェストと受信した時間のタイムスタンプ、受信者のＩＤ等に対して電子署名を添付した受信通知を発信する。

【００７６】

この構成をとるのは、例えば、受信側の端末が故障していたり、通信回線が不通となっていた場合には、通信内容が受信者に着信しない可能性がある。そのため、受信者は受信通知を発信することが望ましい。しかし、従来の受信通知（例えば、Ｅメールの開封通知）では、途中で悪意ある者が、成りすまして同様の通知を送ることが可能となるため、安全な受信通知とは言えない。本実施の形態の暗号情報復号化装置３は、上記受信通知発信部３ｃを設けている。これにより機密情報を送受する同報通信において、受信者本人が電子署名を添付した受信通知を情報中継装置に発信することができ、情報中継装置ではこの電子署名を検証することにより、メンバーリストに登録されたメンバーの１人に確実に配信できたことを確認できる。

【００７７】

次に、暗号情報復号化装置３の第３の実施の形態として、図９に示すように第１または第２の実施の形態の暗号情報復号化装置に、さらに複数パーツ受信部３ｄを備える構成をとる。

複数パーツ受信部３ｄは、図８に示すように同報通信文の内容より、情報保管装置５にパーツの一部分が転送されているか判断し、もし、パーツが転送されている場合、情報保管装置５に問い合わせ、各パーツの送信に最適なプロトコル（例えば、ＨＴＴＰプロトコルやＦＴＰプロトコル）を利用してパーツを取得する。また、本実施の形態の復号化部３ｂは、暗号化情報が複数のパーツで構成されている場合には、個々のパーツごとに復号化処理を行うように動作する。

なお本実施の形態は、同報通信文が複数のパーツで構成され、前述の暗号情報作成装置２により、パーツのうちのいくつかが情報中継装置４から参照できる情報保管装置４に送信される場合に対応するものである。

【００７８】

本発明の暗号情報復号化装置の第４の実施の形態は、図９に示すように第１ないし第３の実施の形態のいずれかの暗号情報復号化装置３に、さらに同報通信安全性検証部３ｅを備える構成をとる。

同報通信安全性検証部３ｅは、その機能の１つとして送信者がメンバーリストに登録されているメンバーかどうかを検証するように動作する。この検証の際には、後述のリスト取得保存部３ｆよりメンバーリストを取得して送信者を確認する。また、ネットワーク上に配置されたメンバーリストに関する情報を登録したリソースデータベースにアクセスし（例えばＬＤＡＰなどのプトロコル）を利用して、メンバーリストの中に含まれている送信者かどうかを、問い合わせるようにしてもよい。また、後述の情報中継装置に備わる同報通信安全性検証部と同様の機能をさらに備えてもよい。

【００７９】

本発明の暗号情報復号化装置の第５の実施の形態は、図９に示すように第１ないし第４の実施の形態のいずれかの暗号情報復号化装置３に、さらにリスト取得保存部３ｆを備える構成をとる。

【００８０】

リスト取得保存部３ｆは、メンバーリストをネットワーク上に配置されたリソースデータベースに保存されたメンバーリストを、同報通信と同じ、または、異なるプロトコル（例えば、同報通信でＳＭＴＰを利用する場合には、ＨＴＴＰな

ど）を利用して取得する。もしくは、転送されてきたメンバーリストを記憶装置（図示せず）に保存し、必要なときに保存先からメンバーリストを読み込むことにより取得する。

また、暗号情報復号化装置３がすでにメンバーリストを保存している場合には、リスト取得保存部３ｆは、メンバーリストが最新バージョンか確認するように動作する。例えば、メンバーリストの最新バージョンに関する情報が保存されたネットワーク上に配置されたデータベースに、同報通信と同じまたは、異なるプロトコル（例えば、同報通信でＳＭＴＰを利用す場合には、ＬＤＡＰ、ＯＣＳＰなど）を利用して、最新のメンバーリストのバージョンを問い合わせ確認する。

【００８１】

また、リスト取得保存部３ｆは、前述のメンバーリスト管理装置１の実施の形態で説明したメンバーリストの正当性を検証する機能を備え、メンバーリストの取得時にメンバーリストの正当性を検証する。

さらに、前述の暗号情報作成装置の実施の形態で説明した公開鍵や電子署名に利用される秘密鍵の有効性を検証する機能を、復号化部３ｂ、リスト取得保存部３ｆに備え利用する形態としてもよい。これらの機能をさらに備えることで、安全性がさらに向上する。

以上、本発明の暗号情報復号化装置の各実施の形態を説明した。

【００８２】

図１０は、本発明の情報中継装置の第１から第６の実施の形態を包含し表している。

まず、本発明の情報中継装置の第１の実施の形態を説明する。

本実施の形態は、チームマスターによって管理される配信先リストを保存・管理する配信先リスト管理部４ａと、転送されてきた暗号情報を、配信先リストに含まれる被配信メンバーに転送するために複製する情報複製部４ｂと、複製された暗号情報をそれぞれの被配信メンバーに送信する送信部４ｃとから構成される。

【００８３】

配信先リスト管理部４ａは、配信リストを保存・管理する機能と、メンバーリ

ストを取得し保存する機能と、メンバーリストを取得する際に、メンバーリスト管理装置の実施の形態で説明したメンバーリストの正当性を検証する機能と、メンバーリストと配信リストに含まれるメンバーを一致させる機能を備える。なお、配信先リスト管理部４ａがメンバーリストを参照して配信先リストを設定する場合には、メンバーリストが最新バージョンであるか確認する機能をさらに備える。例えば、メンバーリストの最新バージョンに関する情報が保存されたネットワーク上に配置されたデータベースに、同報通信と同じまたは、異なるプロトコル（例えば、同報通信でＳＭＴＰを利用す場合には、ＬＤＡＰ、ＯＣＳＰなど）を利用して、最新のメンバーリストのバージョンを問い合わせるようにしてもよい。

【００８４】

本発明の情報中継装置の第２の実施の形態は、第１の実施の形態の情報中継装置４に、リスト正当性確認部４ｄをさらに備える構成をとる。

リスト正当性確認部４ｄは、メンバーリストを取得した場合に、メンバーリスト正当性の検証を行う。このメンバーリストの正当性の検証を行なう機能は、前述のメンバーリスト管理装置１の実施の形態で説明したとうりである。

【００８５】

本発明の情報中継装置の第３の実施の形態は、第１または第２の実施の形態の情報中継装置４に、付加情報添付部４ｃをさらに備える構成をとる。

付加情報添付部４ｃは、チームマスターまたは情報中継装置４の管理者による各種情報（サービス情報、管理情報等）を暗号情報に添付するものである。この付加情報を添付する機能により、被配信メンバーに幅の広いサービスを提供することができる。

【００８６】

本発明の情報中継装置の第４の実施の形態は、第１ないし第３の実施の形態のいずれかの情報中継装置４に、同報通信安全性検証部４ｆをさらに備える構成をとる。

【００８７】

同報通信安全性検証部４ｆは、第１の機能としてメンバーリストの同一性を検

証する機能をもつ。例えば、送信側の端末が故障していたり、通信回線が不通となっていた場合には、最新のメンバーリストが送信者に行き渡っていない可能性がある。同報通信安全性検証部４ｆは、より同報通信の安全性を高めるために、転送されてきた暗号情報の暗号化時に利用したメンバーリストと、サーバが転送時に利用する配信先リストを作成するために用いたメンバーリストとの同一性の検証を行う。

【００８８】

例えば、メンバーリストのバージョンＮｏ．やチームマスターがメンバーリストを作成したときの時間（例えば、タイムスタンプなどが付加されていた場合）などの情報を利用して、メンバーリストが同一のものかを検証することができる。また、別の手法としては、メンバーリストに添付された電子署名者が同一かどうかを検証することにより、同一性検証を行うことができる。また、別の手法としては、メンバーリストに対してハッシュ関数を利用してメッセージダイジェストを比較することにより、同一性検証を行うことができる。

【００８９】

また、同報通信安全性検証部４ｆは、第２の機能として同報通信送信者を検証する機能をもつ。従来の同報通信は、情報中継装置４の管理者が情報の中身を見ることができたため、例えば、中傷・誹謗情報が流れているか否かなどの、内容を検査することができた。しかし、本発明の方式では、サーバの管理者が情報の中身を見れない仕組みを実現しているため、この情報中継装置４を不正に利用される可能性がある。そこで、同報通信安全性検証部４ｆは、情報受信を拒否する情報端末（例えば、ＩＰアドレスなどによって識別できる）、または、利用者の識別情報（例えば、メールシステムの場合には、メールアドレスや、信頼できる認証局より発行された証明書などによって識別できる）が含まれる受信拒否情報を取得し、情報中継装置４に転送されてきた情報の送信者または、送信端末が、受信拒否情報に含まれているか否かを検証する機能をもつ。なお、受信拒否情報には、例えば、過去にスパムメールを発した個人のメールアドレスや、セキュリティレベルが低く本人識別が正当な手順をもって行われていない可能性がある端末のＩＰアドレスやネットワークアドレスのリストが含まれている。

【００９０】

また、同報通信安全性検証部４ｆは、第３の機能として同報通信内容を検証する機能をもつ。これは、同報通信の安全性を高めるために、送信者や通信内容についても検証を行なうものである。暗号情報の送信者がメンバーリストに含まれた者かどうかの検証や、転送されてきた情報の中に悪意あるプログラムやデータ列が含まれているかどうかの検証を行なう。

【００９１】

また、同報通信安全性検証部４ｆは、第４の機能として複数パーツからなる暗号情報のうち、情報保管装置に保存され暗号情報復号化装置から参照されるパーツが間違いなく情報保管装置に転送されたかを検証する機能をもつ。転送されてきた暗号情報を参照して複数のパーツで構成される暗号情報のうち、一部を別の情報保管装置に転送しているか判別し、一部が別の情報保管装置に転送されている場合、確実に転送されたかを検証する。

さらに、前述の暗号情報作成装置の実施の形態で説明した公開鍵や電子署名に利用される秘密鍵の有効性を検証する機能は、同報通信安全性検証手段４ｆに備えられ利用される形態もある。

【００９２】

本発明の情報中継装置の第５の実施の形態は、第１ないし第４の実施の形態のいずれかの情報中継装置４に、同報通信内容保存部４ｇをさらに備える構成をとる。

同報通信内容保存部４ｇは、転送されてきた情報、または、情報の一部、または、それらの情報に添付情報を添付して保存する。例えば、メールシステムにおけるメールサーバに障害が発生した場合や、受信者の端末が故障していた場合には、送信された情報であっても正確に受信されない可能性がある。また、音声チャットにおいて通信回線の都合上、音声が途切れ途切れになる場合などもある。このように送信側が送ったデータと受信側が受け取ったデータが一致しなかった事態が発生しても、同報通信内容保存部４ｇによる保存機能により安全に保存しておき、必要になったときに再度確認したり再取得することができる。

【００９３】

本発明の情報中継装置の第６の実施の形態は、第１または第５の実施の形態のいずれかの情報中継装置４に、同報通信自動開設部４ｈをさらに備える構成をとる。

同報通信自動開設部４ｈは、同報通信をサーバ管理者の手動の許可を得ることなく自動的に開始するため、サーバ管理者が開設受付の際に開設要求者が満たすべき項目を提示するための開設要求項目提示機能と、開設要求者が転送してきた開設受付要求が、開設要求項目を満たし、開設を許可するか否かをを判断する開設許可判断機能と、開設が決定されると、開設要求者をチームマスターとし、チームマスターが指定したメンバーに同報通信が可能になるよう開設設定を行う同報通信開設設定機能をもつ。

【００９４】

従来の同報通信システムは、事前に情報中継装置の管理者が、開設に伴う作業を行う必要があった。例えば、配信リストの設定や、ＩＣカードを配布したり、情報中継装置に公開鍵を登録したりする作業が必要であった。また、暗号同報通信は、延々と続く通信ではなく、例えば、１時間の音声チャット、３通の契約書ファイルの転送といったように、必要なときに最小限の時間で利用する通信であることも多いと考えられる。その場合、情報中継装置４の同報通信の開始や削除に関する作業負担が非常に大きくなる。また、ミスの発生や悪意のある管理者の存在などの危険性があるため、このような人による手動の設定はできるだけ必要としないシステムが、安全上望ましい。そこで、本実施の形態の情報中継装置４は、サーバ管理者の手動の設定を必要とすることなく、一定の利用条件（例えば、利用時間に比例する料金の支払い等）を満たせば、自動的に同報通信を開始できる機能を提供する。

【００９５】

さらに、同報通信自動開設部４ｈは、開設要求者が転送してきた開設受付要求が、正確な要求であるかどうかを検証する開設要求確認機能を備えてもよい。例えば、課金項目にクレジットカードが記されていた場合に、クレジットカードの番号がきちんと登録され課金可能な状態であるかを検証する。この検証の際に、情報中継装置４に検証に利用するデータが無い場合には、ネットワーク上に配置

され所定のデータをもつデータベースやサーバ等に問い合わせる。

【００９６】

第６の実施の形態の情報中継装置４に、同報通信のメンバーの脱退要求を受け付ける脱退要求受付部（図示せず）を備えてもよい。

例えば、加入する意志がないのに、勝手にメンバーリストに登録されて、不要な情報や中傷・誹謗情報ばかりが転送されるという危険性がある。本形態の情報中継装置４では、脱退要求受付部は、同報通信のメンバーが、情報中継装置に対して同報通信から脱退するという脱退要求が来た場合には、該メンバーへの転送をとりやめ、その故をチームマスターに連絡する脱退要求受付部を備えることを特徴とする。また、脱退要求が、間違いなく脱退要求メンバー本人が作成した転送中止要求かどうかを調べるために、電子署名やシェイクハンドなどの本人確認手法を利用することができる。

以上、本発明の情報中継装置の各実施の形態を説明した。

【００９７】

次に、本発明の同報通信システムの実施例１として、第三者が運用する情報中継装置を利用して、証券会社が証券ニュースを会員に配信する例を説明する。図１１に示す実施例１では、メールシステムの安全な同報通信を実現するため、メーリングリスト・サーバとＷＷＷサーバを用いて本発明の情報中継装置の機能を実現している。このメーリングリスト・サーバが第三者によって運用されている。

【００９８】

第三者が運用するメーリングリスト・サーバと連動したＷＷＷサーバで、ＷＷＷサーバには、同報通信の開設にメーリングリスト・サーバの管理者が設定した、開設要求者が満たすべき項目を示したホームページが保存されている。証券会社は、サービスを自動開設するために、ＳＳＬ（Secure Socket Layer）通信を利用してこのホームページをダウンロードし、ブラウザに表示された項目に対応するフォーム内に必要事項を入力する。本実施例１では、名前、クレジットカード番号と１０００人まで同報通信できるサービスを要求することを記載して、送信ボタンを押し、ＷＷＷサーバに転送する。

【００９９】

ＷＷＷサーバ上で稼動するプログラム（例えば、ＣＧＩ）として実装された同報通信自動開設部４ｈの開設許可判断機能は、ＳＳＬ通信で確認したアクセスした者の証明書と、名前、クレジットカードＮｏ．、「１０００」の４つデータを利用して、開設を許可するべきか否かを判断する。実施例１では、クレジットカードＮｏ．をクレジットカードサービス会社に問い合わせ、カード保持者と証明書の所有者が一致するかどうかを検証し、一致した場合には、開設を許可する旨を知らせるページを加入要求者に再度転送する。一致しない場合には、開設が拒否された旨を知らせるページを加入要求者に再度転送する。

【０１００】

開設を許可した場合には、メーリングリストサーバ上で稼動するプログラムとして実装された同報通信自動開設部４ｈの同報通信開設設定機能により、加入要求者がチームマスターとなって管理する同報通信のためのメーリングリストアドレスを新規に設定する。また、このメーリングリストアドレスに送信されてきた情報を配信するための配信リスト（当初は、空のリスト）を設定する。これらの開設設定が終了するとメーリングリストサーバは、チームマスターに対して、開設設定が成功終了した旨を通知するメールを転送する。

【０１０１】

実施例１におけるメンバーリスト管理装置１は、例えばＪＡＶＡのアプレットとして実装され、ホームページのなかに組み込まれて、ＷＷＷサーバに保存されている。チームマスターは、メンバーリストを作成する際に、ＳＳＬ通信を利用してダウンロードされてくるアプレットを用いて、設定したいメンバーリストの管理を行う。本実施例１におけるメンバーリストは、チームマスターリスト、レポーターリスト、受信者リストの３つのリストで構成されている。チームマスターリストには、チームマスター以外にチームを管理できるサブマスターを設定し、レポーターリストには、証券ニュースを書く記者を登録し、チームマスターの電子署名を行って、情報中継装置４に再度転送する。情報中継装置４は、メンバーリストが間違いなくチームマスターによって作成されているかを電子署名を検証した後、配信リストを設定する。本実施例１での配信ルールは、レポーターリ

ストのメンバーから転送されてきた同報通信情報を受信者リスト（メンバーリストに含まれる）に登録されたメンバー分複製し、登録するように設定されている。

【０１０２】

受信者は、基本的に毎月の課金が行えるユーザであれば自動的に加入してもらえるよう実装するため、本実施例１では、メンバーリスト管理部１の加入要求受付部１ｄを利用する。チームマスターによって設定されたメンバーリストに含まれるチームマスターリストには、複数のサブマスターが設定されている。サブマスターもまた、証券会社の社員であり、このサブマスターは、受信者リストの管理を担当している。サブマスターは、WWWのページとして実装された加入要求受付部１ｄの加入要求項目設定機能を、ＳＳＬ通信を利用してダウンロードする。この際、WWWサーバは、ＳＳＬ通信で取得できるサブマスターの証明書を見て、サブマスター本人の識別・認証を行う。WWWページ内のフォームの各項目を埋めていくことによって、加入要求項目を設定する。本実施例では、サービスの契約同意書、課金項目、メールアドレスとメールアドレスを含む証明書を提示してもらう旨を指定し、さらに、加入要求者の加入要求を暗号化するためのサブマスターの公開鍵を指定して転送する。

【０１０３】

上記証券ニュース配信サービスへの加入要求者は、WWWページに埋め込まれたＪＡＶＡアプレットとして実装された加入要求受付部１ｅの加入要求項目提示機能を利用して、まず、契約同意書に自分の秘密鍵を利用して電子署名を行い、また、課金項目、メールアドレスを入力する。これを転送する際には、これらの機密情報（特に、課金に関する情報：クレジットカードＮｏ．や銀行の口座番号等）は、WWWサーバやメーリングリストサーバの管理者に見えてはいけないので、サブマスターの公開鍵を取得して暗号化を行ってから、WWWサーバに転送する。また、以上の通信は、ＳＳＬで行われているため、認証を行う際に証明書も確認することができる。

【０１０４】

多数の加入要求者からの加入要求は、WWWサーバに暗号化された加入要求情

報として保存されている。実装例１では、加入要求受付部１ｅの加入許可判断機能を実装したプログラムは、WWWサーバにアクセスし、暗号化された加入要求情報を取得し、各項目がサービス加入を許可できるよう満たされているかどうかを判断する。例えば、鍵有効性検証機能を利用して、公開鍵と秘密鍵がまだ有効であるかを検証する。判断の結果、加入を許可または、拒否した旨を示す通知メールを加入要求者に対して転送する。このプログラムは、さらにメンバーリスト管理装置を自動操作することができる。

【０１０５】

許可が出された加入要求に対しては、メンバーリスト管理装置１を利用して、WWWサーバに保存されたメンバーリストを、メンバーリスト取得保存部１ｃを利用して取得し、メンバーリストのうち、受信者リストに加入要求者をを登録する。このメンバーリストには、サブマスターとして登録されているサブマスターの秘密鍵を用いてこの受信者リストに対して電子署名を添付し新メンバーリストとして、再度WWWサーバに転送する。WWWサーバでは、前述のメンバーリストの正当性を検証する機能を利用してメンバーリストの正当性を確認し、さらに公開鍵や電子署名に利用される秘密鍵の有効性を検証する機能を利用してメンバーリストに含まれている公開鍵がすべて有効であるかを検証する。これらの検証結果が肯定であれば、配信先リスト管理部４ａを利用して配信先リストを更新する。また、レポーターリストに含まれているメンバーに対しては、最新のメンバーリストをリスト送信部１ｄ（実施例では、ＳＭＴＰプロトコルを利用して実装されている）を利用して、送信しておく。

【０１０６】

記者が証券ニュースを作成する端末は、汎用的なコンピュータ（本実施例１では、ノートブックパソコン等）などに、電子メールソフトウェアが組み込まれている。この電子メールソフトウェアを利用して作成した記事をメーリングリストのアドレスを指定して転送しようとする。この時、この電子メールソフトウェアと連動するプラグイン・ソフトウェアとして実装された暗号情報作成装置２は、宛先検査部２ｃを利用して、メーリングリストアドレスがメンバーリストの存在する情報中継装置４に転送しようとしていることを確認する。

【０１０７】

この場合、プラグイン・ソフトウェアは、まず、リスト取得保存部２ａを利用して、端末のパソコンに存在するメンバーリストのバージョンが最新のバージョンかを検証する。これは、ネットワーク上にＸ．５００の標準に基づいて構築されたリソースデータベースに対して最新のバージョンを、ＬＤＡＰを利用して問い合わせる。最新のバージョンでなかった場合には、リソースデータベースに登録された最新バージョンの所在場所から最新のメンバーリストを取得する（実施例では、WWWサーバより、ＳＳＬ通信を利用して取得する）。

【０１０８】

暗号情報作成装置２では、メンバーリストの正当性を検証する機能を利用してメンバーリストの正当性を確認後、メンバーリストに含まれる受信者リストのメンバーの公開鍵を利用して暗号化部で、暗号化を行う。この際に、電子署名付加機能は、記者が保有する秘密鍵を記録したＩＣカードから、この記者の秘密鍵を取得し、作成された記事に対して電子署名を添付する。この署名により、受信者は、どの記者が書いた記事かを確認でき、記事の信頼性を確かめることができる。また、記事を配信した記者は、記事を作成したこと否認できなくなる。

【０１０９】

メーリングリストのアドレスに送信されたメーリングリストは、まず、同報通信安全性検証部４ｆを利用して送信された情報の署名添付者（本実施例１では、記者）が、間違いなくメンバーリストのうちのレポーターリストに含まれているか確認する。また、メンバーリストの同一性を検証する機能を利用して、メンバーリストのバージョンが異なっていないかを検証する。検証した結果、メンバーリストのバージョンが異なる場合には、その旨を明示した情報と同報通信情報をこの記者に対して返信する。以上の検証の結果、すべて正常であれば、情報複製部４ｂを利用して暗号情報を複製し、メンバーリストの受信者リストに含まれるメンバーに対して、ＳＭＴＰプロトコルで実装された送信部４ｃを利用して送信する。

【０１１０】

受信者の電子メールソフトウェアに組み込まれたプラグイン・ソフトウェアと

して実装された本発明の暗号情報復号化装置は、復号化部３ｂの電子署名を検証する機能を利用して改竄の有無および情報作成者を確認して、送信者が証券会社の記者であることを確認する。確認後記事を復号化して、記事を読むことができる。記事を無事復号化できた時点で、受信通知発信部３ｃを利用して、情報中継装置４に対して受信通知を送信する。

【０１１１】

なお、本実施例におけるＪＡＶＡアプレットが本当に悪意がないかどうかをチェックするには、ＪＡＶＡアプレットに添付された電子署名を確認することによって、検証できる

以上、実施例１における各装置の動作を説明した。

【０１１２】

次に、本発明の同報通信システムの実施例２として、複数の企業間にまたがるメンバー間（この集合を、チーム００１とする）で見積もりや商談等の機密情報を同報通信して行う場合に利用される例を説明する。図１２に示す実施例２では、情報中継装置としてメーリングリストサーバを利用する。

【０１１３】

チーム００１のチームマスターは、汎用的なデスクトップコンピュータのＯＳ上に実行ファイルとして実装されたメンバーリスト管理装置１を利用して、機密情報を同報通信するメンバーリスト管理を行う。リスト取得保存部１ｃを利用してメンバーリストを取得し、リスト作成・変更ＧＵＩ画面を開く。このＧＵＩ画面には、チーム００１のメンバーの一覧と、公開鍵管理部１ｂを利用して端末にある公開鍵のデータベースにアクセスし、保存されている公開鍵の一覧を表示している。

【０１１４】

チーム００１のチームマスターは、公開鍵一覧から、チームに加入するメンバーの公開鍵を選択し、チーム００１のメンバー一覧に追加する。また、公開鍵管理部１ｂが提供するネットワークアクセス機能を利用して、ネットワーク上の認証局が提供するディレクトリーサービスにアクセスし、端末になかった公開鍵で新たにチーム００１に追加したいメンバーの公開鍵を取得し、この公開鍵をメン

バーリストに加える。

【０１１５】

ＧＵＩ画面には、ＯＫボタンが表示されており、チーム００１のメンバーを変更し終わったら、このＯＫボタンを押す。この時点で、公開鍵や電子署名に利用される秘密鍵の有効性を検証する機能は、メンバーリストに含まれるそれぞれの公開鍵が含まれる証明書を発行した認証局のディレクトリサービスにＬＤＡＰプロトコルを利用してアクセスし、この公開鍵が有効であるかどうかを検証する。検証の結果、無効の公開鍵があれば、その旨をダイアログに表示して、チームマスターに通知する。すべて有効であれば、タイムスタンプと、メーリングリストのアドレスとチームＩＤとチームマスターの識別名で構成されるメンバーリストを作成し、このメンバーリストの全体のデータをハッシュ関数のＭＤ５を利用して圧縮し、圧縮データを生成する。

【０１１６】

次に、チームマスターの秘密鍵にアクセスし、チームマスターがダイアログボックスより入力したパスワードを利用したパスワード復号化（実施例では、共通鍵暗号方式ＲＣ２を利用して実装されたパスワード復号化を利用する）を行う。その結果取得した、チームマスターの秘密鍵を利用して、圧縮データを公開鍵暗号方式ＲＳＡで、暗号化することにより、電子署名を作成する。このメンバーリストと電子署名を情報中継装置４にＳＭＴＰプロトコルを利用してメールとして転送する。

【０１１７】

情報中継装置４では、配信先リスト管理部４ａのメンバーリスト取得機能を利用して、受信したマルチパート（ＭＩＭＥ（Multipurpose Internet Mail Extensions））のフォーマットで構成されたＳＭＴＰメールの中身を解析し、Ｃｏｎｔｅｎｔ－Ｔｙｐｅより判断したメンバーリスト部分を抽出して、リスト正当性確認部４ｄに入力する。リスト正当性確認部４ｄは、メンバーリストの署名者として間違いなくチーム００１のチームマスターの電子署名が添付されていることを確認し、配信先リスト管理部４ａを利用して、配信先リストの受信者を変更する。その後、変更されたばかりの配信先リストの受信者に対して、メンバーリス

トと電子署名をＭＩＭＥフォーマットごと複製し、配信先リストの各受信者に対して転送する。

【０１１８】

汎用的なデスクトップコンピュータ上にインストールされたメーラーとして動作する暗号情報作成装置２は、メンバーリストが含まれたメールを受け取った場合には、ＭＩＭＥのＣｏｎｔｅｎｔ－Ｔｙｐｅより、このメールが同報通信におけるメンバーリストであることを識別する。その時点で、メーラーは、メンバーリストと電子署名を抽出し、リストの正当性を検証する機能を利用して、メンバーリストの正当性を確認した後、リスト取得保存部２ａを利用して保存しておく。

【０１１９】

チーム００１に含まれるメンバーが、汎用的なデスクトップコンピュータ上で可動する一般的な実行プログラムとして実装された暗号情報作成装置２の同報通信情報作成機能を利用して、見積書と契約書の２つの添付ファイルを含むメールを作成した後、送信ボタンを押すと、宛先検査部２ｃが送信先アドレスをチェックし、送信先アドレスが端末に保存されている複数メンバーリストのうち、送信先アドレスのために私用するメンバーリストがあるかを検査する。

【０１２０】

メンバーリストがあった場合には、この添付ファイルとメールを、メンバーリストの公開鍵を利用して暗号化する。その際に、暗号化部２ｂは、それぞれの添付ファイルとメール本文を別々に暗号化し、電子署名も個々に添付する。これらの複数のパーツで構成された情報の内、添付ファイルはそのまま添付せずに、情報保管装置（情報保管サーバ）５に転送する。複数パーツ送信部２ｄは、情報中継装置４のアドレスをもとに、メーリングリストアドレスに対応する情報保管装置５をネットワーク上のデータベースに問い合わせ、２つの添付ファイルを送信すべき情報保管装置４のアドレスと、送信方法（例えば、プロトコルなど）を特定する。

【０１２１】

情報保管装置５は、ＨＴＴＰプロトコル利用したファイル転送を許可する仕組

みであることが分かると、ＨＴＴＰプロトコルを利用して送信する。その際に、情報保管装置５は、ＳＳＬ通信を利用しユーザ認証が可能であるため、ユーザがメーリングリストサーバで行っている同報通信サービスを利用しているメンバーリストに含まれているかを確認することができる。メール本文は２つの添付ファイルの送信とは別に、情報保管サーバのアドレスを添付してアドレスを転送する。

【０１２２】

メーリングリストのアドレスに送信されたメーリングリストは、まず、同報通信安全性検証部４ｆを利用して送られてきた情報の署名添付者が、間違いなくメンバーリストのうちのレポーターリストに含まれているか確認する。また、メンバーリストの同一性を検証する機能を利用して、メンバーリストのバージョンが異なっていないかを検証する。検証の結果、メンバーリストのバージョンが異なる場合には、その旨を明示した情報と同報通信情報を記者に対して返信する。また、同報通信安全性検証部４ｆの同報通信内容検証機能を利用し、通信内容の中に、装置やソフトウェアのバグを利用した悪意あるプログラムやウィルスなどが含まれていないかを検証する。さらに、同報通信安全性検証部４ｆの情報保管装置参照機能を利用して、間違いなく暗号化された２つ添付ファイルが情報保管装置４に転送されて保存されているかを検証する。

【０１２３】

以上の検証の結果、すべて正常であれば、同報通信内容保存部４ｇを利用し、同報通信の内容をメーリングリストサーバに接続されたデータベースに保存しておく。その際に、タイムスタンプとメーリングリストサーバの秘密鍵を利用した電子署名を添付して保存する。また、暗号情報には、情報保管装置４に添付ファイルが保存されていることを確認した事に関する時間と、この暗号情報が、メーリングリストサーバに保存されている事に関する情報を添付して、情報複製部４ｂを利用して暗号情報と添付情報を複製し、メンバーリストの受信者リストに含まれるメンバーに対して、ＳＭＴＰプロトコルで実装された送信部４ｃを利用して送信する。

【０１２４】

出張先のWWWブラウザで、メールを取得しようとしているユーザは、ＪＡＶＡアプレットとして実装された暗号情報復号化装置３を、ダウンロードしブラウザ上でこの暗号情報を受信する。このＪＡＶＡアプレットは、ネットワーク上よりリスト取得保存部３ｆを利用してメンバーリストの最新バージョンを取得し、リストの正当性を検証する機能を利用して、メンバーリストがチームマスター本人によって、作成されたものかどうかを確認する。この暗号情報を取得した際に、まず、復号化部３ｂの電子署名を検証する機能を利用して改竄・情報作成者を確認し、さらに、同報通信安全性検証部３ｅの送信者信頼性確認機能を利用して、メンバーリストに含まれる商談相手であることを確認する。その後、復号化部３ｂを利用し、情報を復号化して暗号情報を見ると情報保管装置５に添付ファイルが送信されていることが判明する。複数パーツ受信部３ｄは、この添付ファイルをＨＴＴＰプロトコルを利用してダウンロードし、それぞれのファイルを再度復号化し、もとの情報を得ることができる。

以上、実施例２における各装置の動作を説明した。

【０１２５】

なお、本発明は、インターネットの他、ＬＡＮやダイアルアップによるネットワークを利用してもよい。

また、本発明のメンバーリスト管理装置を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することによりメンバーリスト管理を行ってもよい。すなわち、このメンバーリスト管理プログラムは、同報通信を行う１以上のメンバーの公開鍵を含むメンバーリストを作成する機能と、前記公開鍵を取得し保存する機能とをコンピュータに実現させる。

【０１２６】

また、本発明の暗号情報作成装置を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することにより暗号情報作成を行ってもよい。すなわち、この暗号情報作成プログラムは、ネットワークを介して、メンバーリストを取得し保存する機能と、同報通信文を取得し、該同報通信文を前記

メンバーリストに含まれる公開鍵を用いて暗号化し暗号化情報とする機能とをコンピュータに実現させる。

【０１２７】

また、本発明の暗号情報復号化装置を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することにより暗号情報復号化を行ってもよい。すなわち、この暗号情報復号化プログラムは、情報中継装置から転送された暗号情報を取得する機能と、前記暗号情報に含まれる暗号化情報を復号化する機能とをコンピュータに実現させる。

【０１２８】

また、本発明の情報中継装置を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することにより情報中継処理を行ってもよい。すなわち、この情報中継処理プログラムは、配信先リストを管理する機能と、転送されてきた暗号情報を複製する機能と、複製された暗号情報を各被配信メンバーに配信する機能とをコンピュータに実現させる。

【０１２９】

また、モバイルネットワーク環境においても同報通信を実現するため、同報通信に必要な本発明のメンバーリスト管理装置、暗号情報作成装置、暗号情報復号化装置を持たない端末を利用しなければならない場合でも、この端末にネットワーク上に配置され各装置のそれぞれの機能を実現するソフトウェアを保存しているソフトウェア保管装置から、各装置の機能を実現するソフトウェアをダウンロードして、端末に内蔵されたコンピュータシステムに読み込ませ実行させることにより、同報通信を行なってもよい。

【０１３０】

なお、ここでいう「コンピュータシステム」とは、ＯＳや周辺機器等のハードウェアを含むものとする。また、「コンピュータ読み取り可能な記録媒体」とは、フロッピーディスク、光磁気ディスク、ＲＯＭ、ＣＤ－ＲＯＭ等の可般媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。

さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムを送信する場合の通信線のように、短時間の間、動的にプログラムを保持するもの、その場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリのように、一定時間プログラムを保持しているものも含むものとする。また上記プログラムは、前述した機能の一部を実現するためのものであっても良く、さらに前述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるものであっても良い。

【０１３１】

以上、この発明の実施形態を図面を参照して詳述してきたが、具体的な構成はこの実施形態に限られるものではなく、この発明の要旨を逸脱しない範囲の設計等も含まれる。

【０１３２】

【発明の効果】

以上詳細に説明したように、本発明によれば、情報中継装置において暗号化された情報を復号化しない仕組みとしたので、情報中継装置の管理者による同報通信の通信内容の漏洩や改竄等の不正を防ぎ、本当に情報を共有する必要のあるメンバーにだけ同報通信内容を共有することができる。

また、本発明によれば、メンバーリスト管理部に加入要求受付部を、そして情報中継装置に同報通信自動開設部を設けたので、同報通信を行う受信者の脱退や、加入に対して迅速に対応でき、同報通信メンバーの動的な変更があっても、誤って同報通信してはいけないメンバーに情報を転送してしまうことを防止できる。

また、本発明によれば、メンバーリストによる管理を行なうので、情報中継装置の管理者が同報通信の被配信メンバーを管理するのではなく、同報通信を行うメンバーの中で被配信メンバーを管理でき、さらにメンバーの管理者に集中する管理負担を軽減することができる。

また、本発明によれば、情報中継装置において同報通信安全性検証部および同報通信内容保存部を設け、暗号情報復号化装置において受信通知発信部および同

報通信安全性検証部を設けたので、多数の被配信メンバーそれぞれが、情報を確実に受信できる。

【図面の簡単な説明】

【図１】　本発明の同報通信システムの仕組みを示す図である。

【図２】　一般的なメンバーリストの例である。

【図３】　複数のリストで構成されたメンバーリストの一例である。

【図４】　本発明のメンバーリスト管理装置の実施の形態を示す図である。

【図５】　リスト作成部の動作フローチャートである。

【図６】　本発明の暗号情報作成装置の実施の形態を示す図である。

【図７】　本発明の同報通信システムにおける暗号化復号化過程を示す図である。

【図８】　本発明の同報通信システムにおける複数パーツ送信および複数パーツ受信の仕組みを説明する図である。

【図９】　本発明の暗号情報復号化装置の実施の形態を示す図である。

【図１０】　本発明の情報中継装置の実施の形態を示す図である。

【図１１】　本発明の同報通信システムを証券ニュース配信システムとして応用した実施例である。

【図１２】　メーリングリストサーバを利用した本発明の同報通信システムの１実施例である。

【図１３】　従来の同報通信システムの仕組みを説明する図である。

【図１４】　特開平７－２４５６０５に開示されている同報通信システムの仕組みを説明する図である。

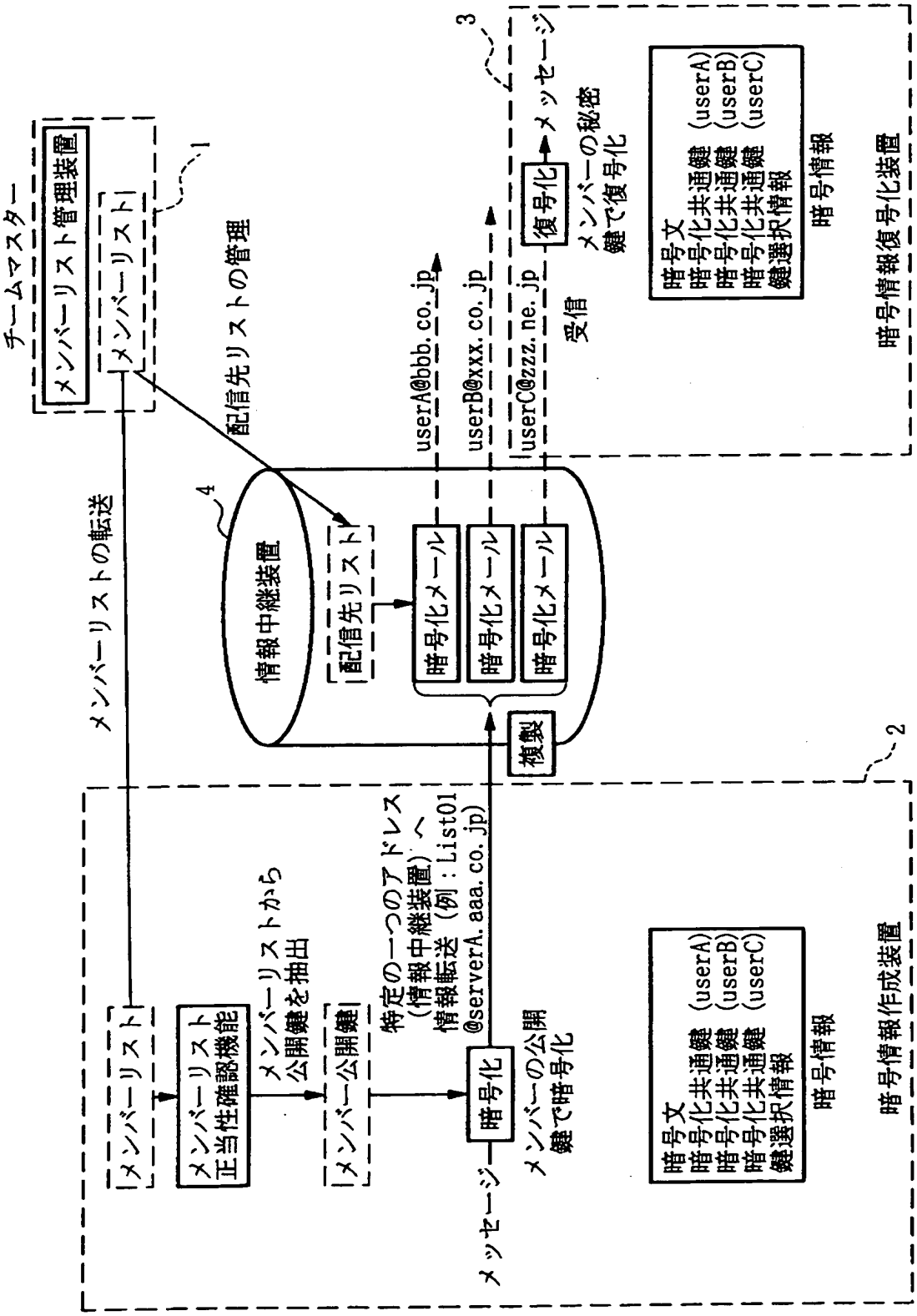
【符号の説明】

１…メンバーリスト管理装置	１ａ…リスト作成部
１ｂ…公開鍵管理部	１ｃ…リスト取得保存部
１ｄ…リスト送信部	１ｅ…加入要求受付部
２…暗号情報作成装置	２ａ…リスト取得保存部
２ｂ…暗号化部	２ｃ…宛先検査部
２ｄ…複数パーツ送信部	３…暗号情報復号化装置

３ａ…暗号情報取得部
３ｂ…復号化部
３ｃ…受信通知発信部
３ｄ…複数パーツ受信部
３ｅ…同報通信安全性検証部
３ｆ…リスト取得保存部
４…情報中継装置
４ａ…配信先リスト管理部
４ｂ…情報複製部
４ｃ…送信部
４ｄ…リスト正当性確認部
４ｅ…付加情報添付部
４ｆ…同報通信安全性検証部
４ｇ…同報通信内容保存部
４ｈ…同報通信自動開設部
５…情報保管装置（情報保管サーバ）

【書類名】　図面

【図１】


チームマスター
メンバーリスト管理装置
メンバーリスト
1
配信先リストの管理
メンバーリストの転送
3
メッセージ
復号化
メンバーの秘密鍵で復号化
受信
暗号文
暗号化共通鍵 (userA)
暗号化共通鍵 (userB)
暗号化共通鍵 (userC)
鍵選択情報
暗号情報
暗号情報復号化装置
4
情報中継装置
配信先リスト
暗号化メール
暗号化メール
暗号化メール
複製
userA@bbb.co.jp
userB@xxx.co.jp
userC@zzz.ne.jp
2
メンバーリスト
メンバーリスト
正当性確認機能
メンバーリストから
公開鍵を抽出
メンバー公開鍵
特定の一つのアドレス
(情報中継装置)へ
情報転送 (例：List01
@serverA.aaa.co.jp)
暗号化
メッセージ
メンバーの公開
鍵で暗号化
暗号文
暗号化共通鍵 (userA)
暗号化共通鍵 (userB)
暗号化共通鍵 (userC)
鍵選択情報
暗号情報
暗号情報作成装置

【図２】

メンバーリスト

チーム101
メンバーX
メンバーY ： メンバーB
Xのデジタル署名

【図３】

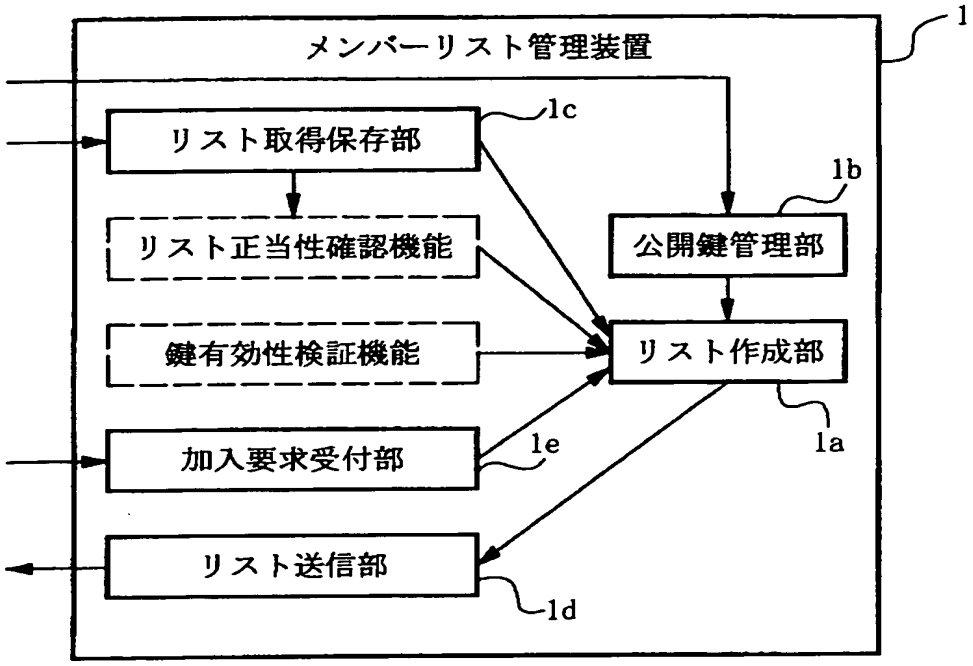
チームマスターリスト

チーム101	
メンバーX	マスター
メンバーY	サブ
メンバーZ	サブ
Xのデジタル署名	

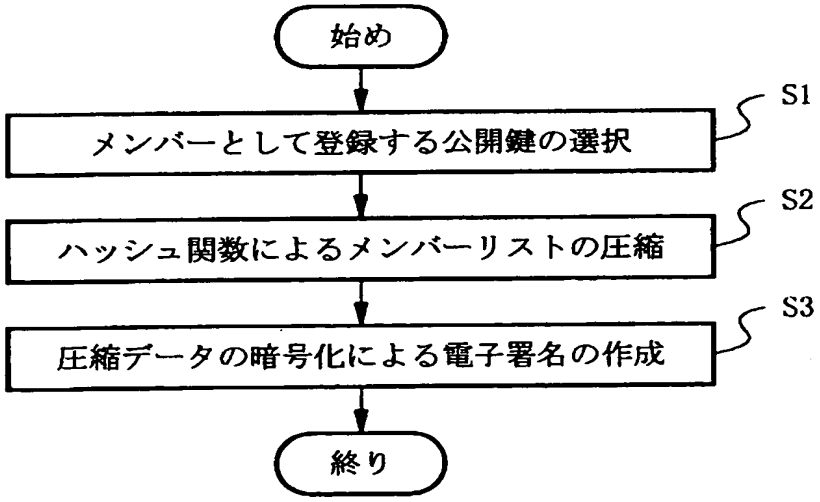
メンバーリスト

チーム101
メンバーX
メンバーY ： メンバーB
Xのデジタル署名

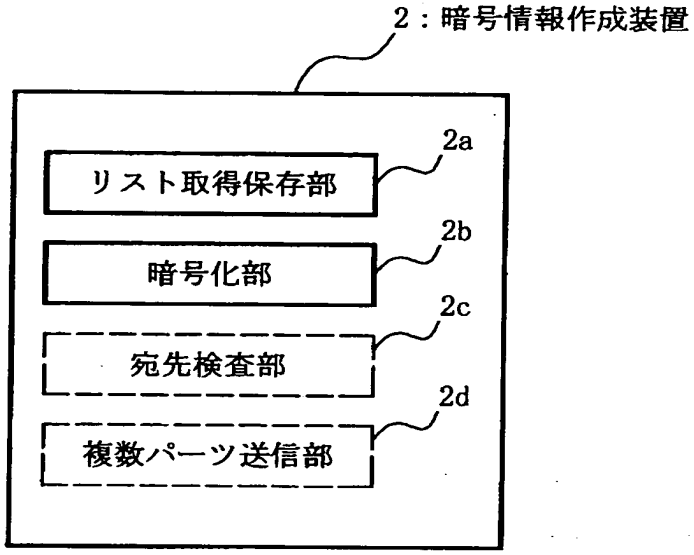
【図４】


メンバーリスト管理装置
1
リスト取得保存部
1c
リスト正当性確認機能
鍵有効性検証機能
加入要求受付部
1e
リスト送信部
1d
公開鍵管理部
1b
リスト作成部
1a

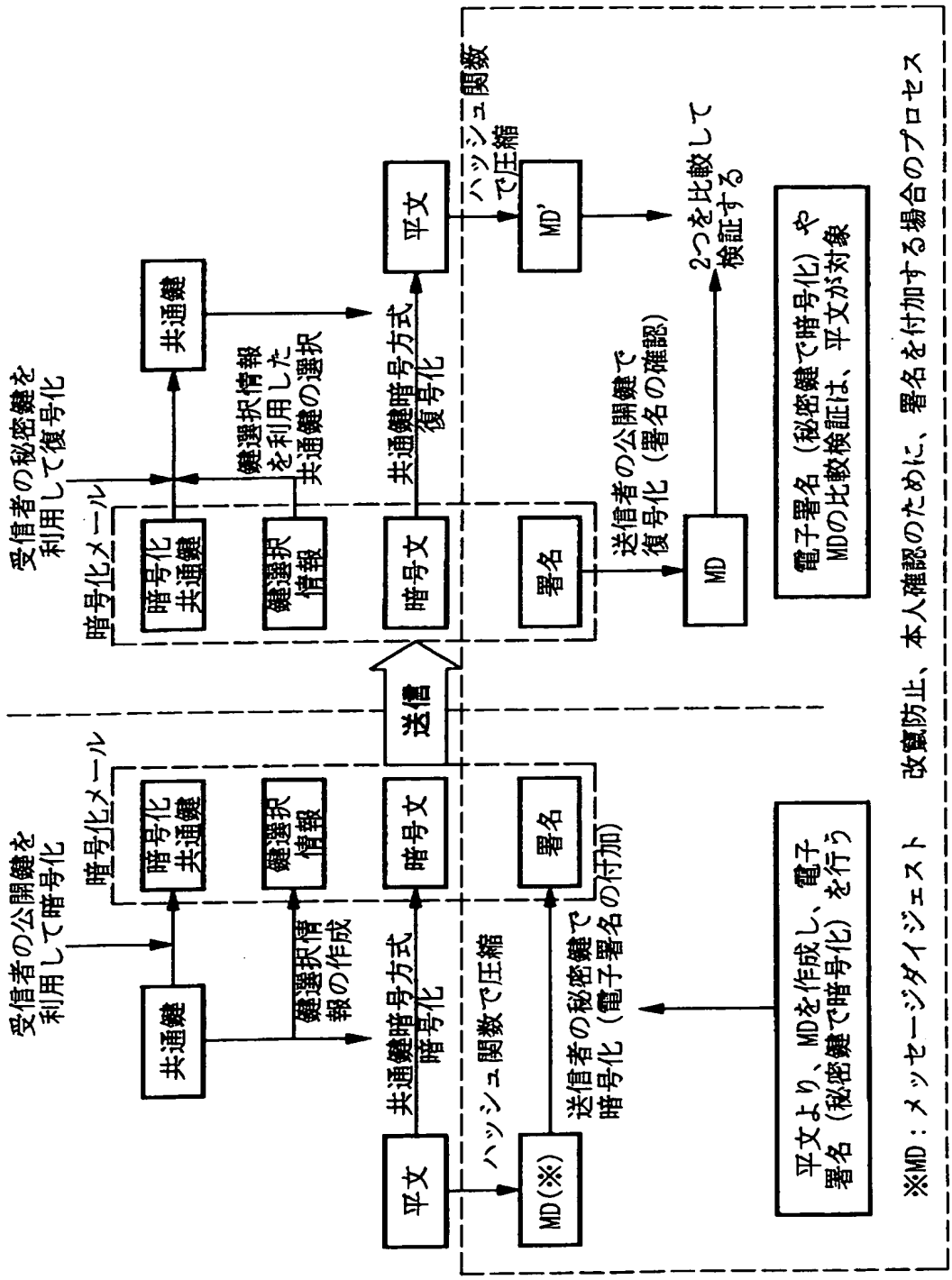
【図５】


始め
メンバーとして登録する公開鍵の選択
S1
ハッシュ関数によるメンバーリストの圧縮
S2
圧縮データの暗号化による電子署名の作成
S3
終り

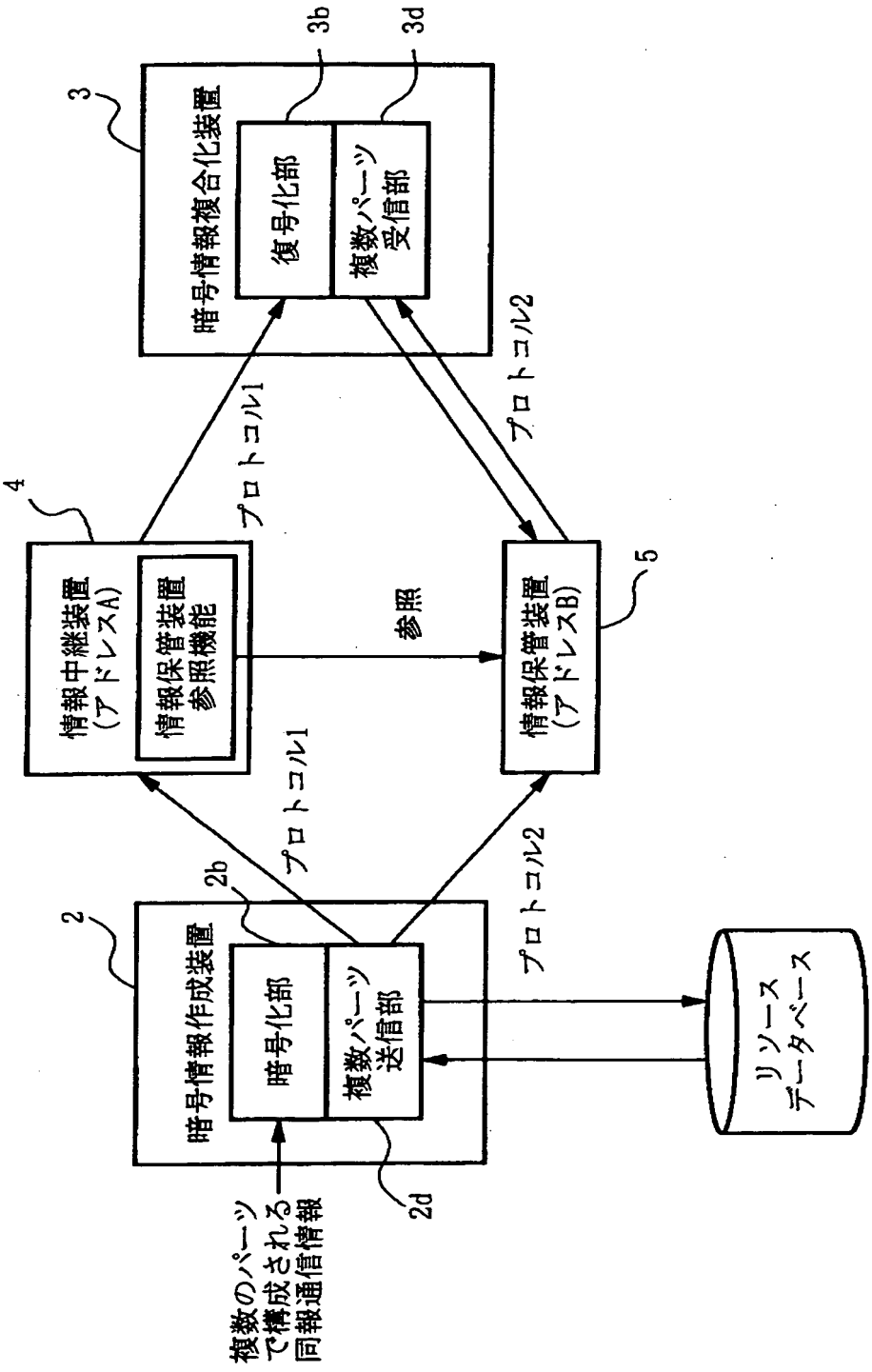
【図６】



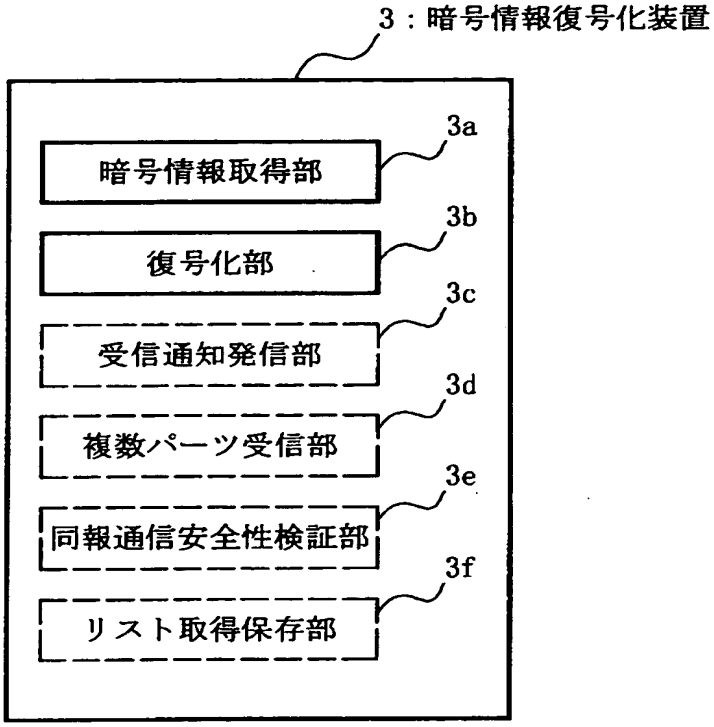
【図７】


受信者の公開鍵を
利用して暗号化
暗号化メール
共通鍵
暗号化
共通鍵
鍵選択情
報の作成
鍵選択
情報
平文
共通鍵暗号方式
暗号化
暗号文
ハッシュ関数で圧縮
MD(※)
送信者の秘密鍵で
暗号化（電子署名の付加）
署名
送信
受信者の秘密鍵を
利用して復号化
暗号化メール
暗号化
共通鍵
鍵選択情報
を利用した
共通鍵の選択
暗号化
共通鍵
鍵選択
情報
共通鍵暗号方式
復号化
暗号文
平文
ハッシュ関数
で圧縮
MD'
送信者の公開鍵で
復号化（署名の確認）
署名
MD
2つを比較して
検証する
電子署名（秘密鍵で暗号化）や
MDの比較検証は、平文が対象
平文より、MDを作成し、電子
署名（秘密鍵で暗号化）を行う
※MD：メッセージダイジェスト　改竄防止、本人確認のために、署名を付加する場合のプロセス

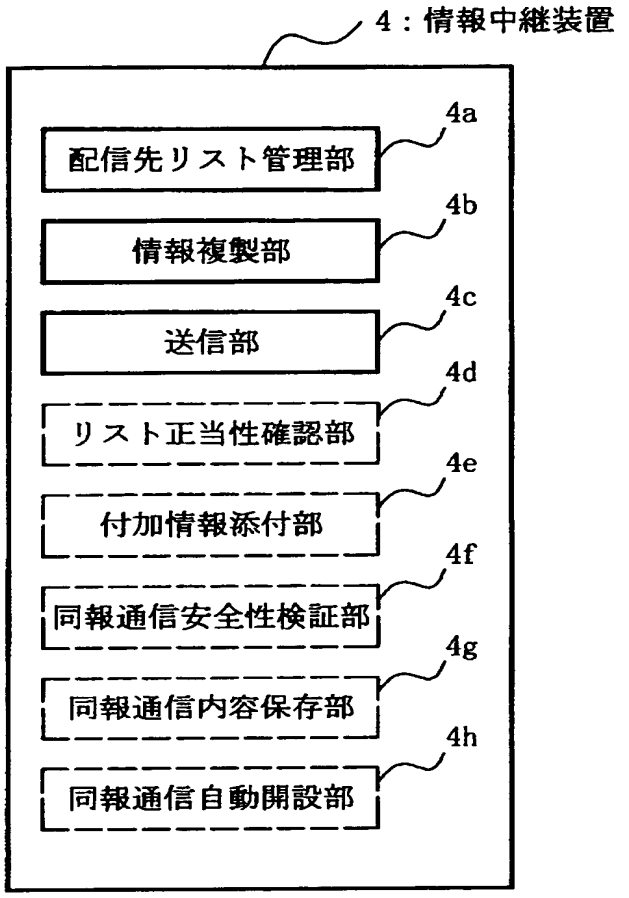
【図８】


3
暗号情報複合化装置
3b
復号化部
3d
複数パーツ
受信部
プロトコル2
プロトコル1
4
情報中継装置
(アドレスA)
情報保管装置
参照機能
参照
5
情報保管装置
(アドレスB)
プロトコル1
プロトコル2
2
暗号情報作成装置
2b
暗号化部
複数パーツ
送信部
2d
リソース
データベース
複数のパーツ
で構成される
同報通信情報

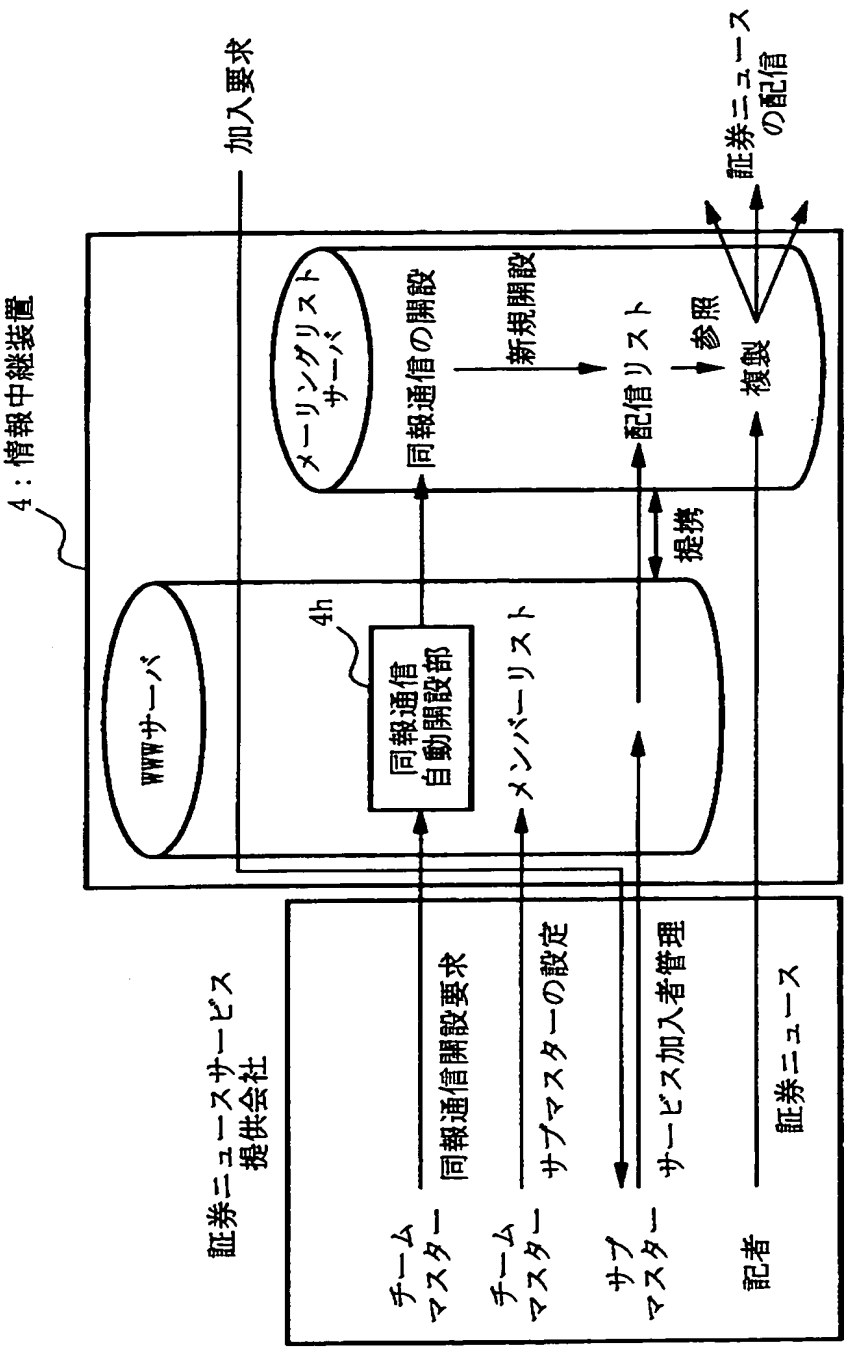
【図９】


3：暗号情報復号化装置
3a
暗号情報取得部
3b
復号化部
3c
受信通知発信部
3d
複数パーツ受信部
3e
同報通信安全性検証部
3f
リスト取得保存部

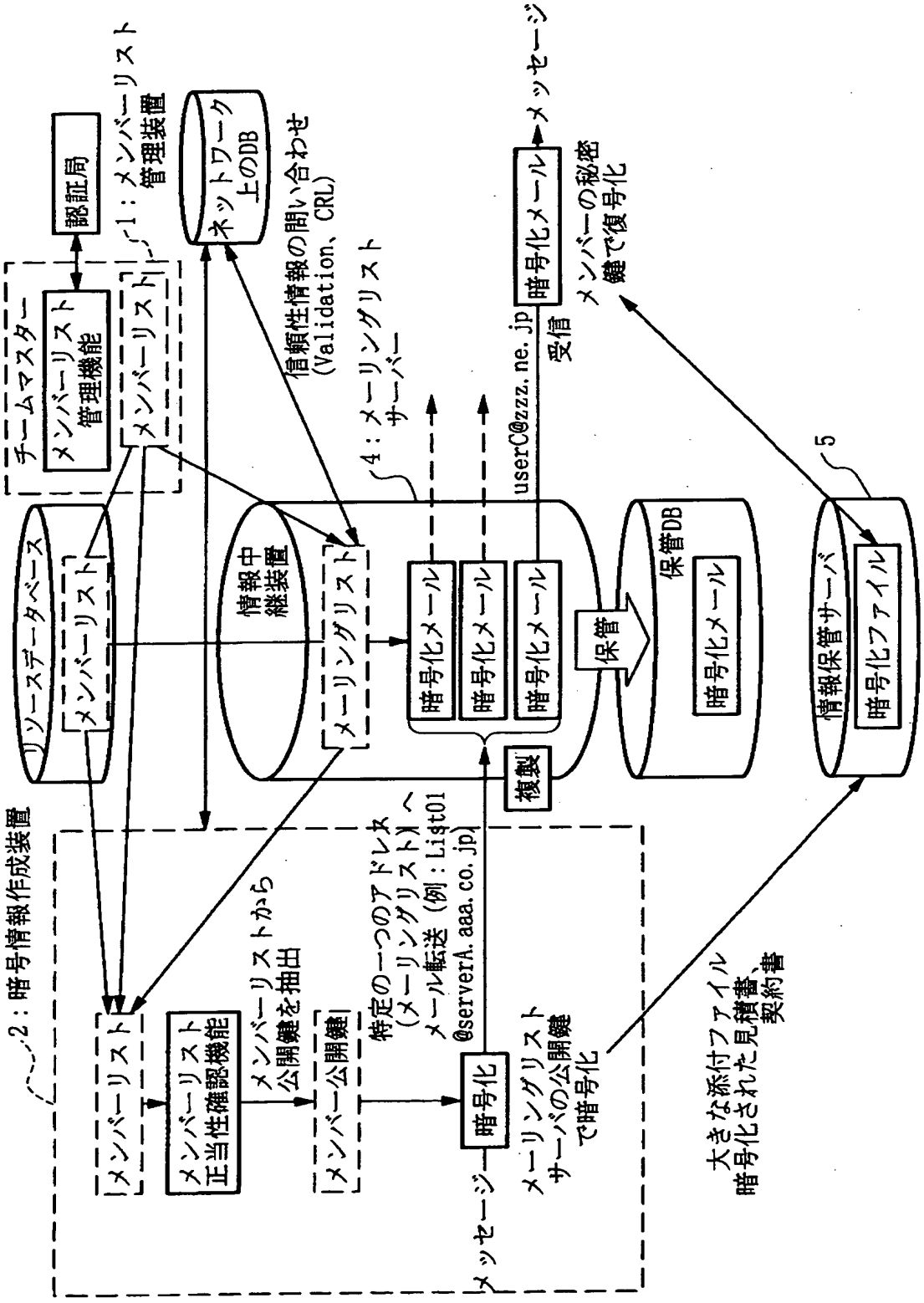
【図１０】


4：情報中継装置
配信先リスト管理部
4a
情報複製部
4b
送信部
4c
リスト正当性確認部
4d
付加情報添付部
4e
同報通信安全性検証部
4f
同報通信内容保存部
4g
同報通信自動開設部
4h

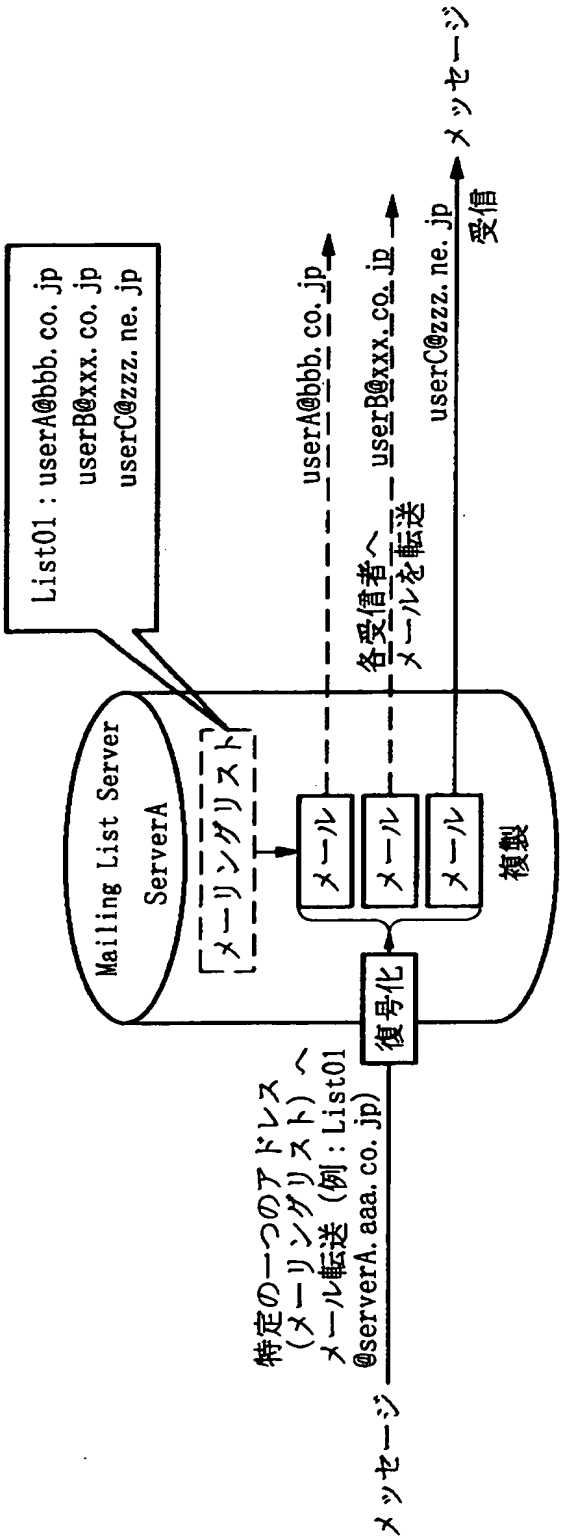
【図１１】


証券ニュースサービス
提供会社
チーム
マスター
同報通信開設要求
チーム
マスター
サブマスターの設定
サブ
マスター
サービス加入者管理
記者
証券ニュース
4：情報中継装置
WWWサーバ
4h
同報通信
自動開設部
メンバーリスト
メーリングリスト
サーバ
同報通信の開設
新規開設
配信リスト
参照
複製
提携
加入要求
証券ニュース
の配信

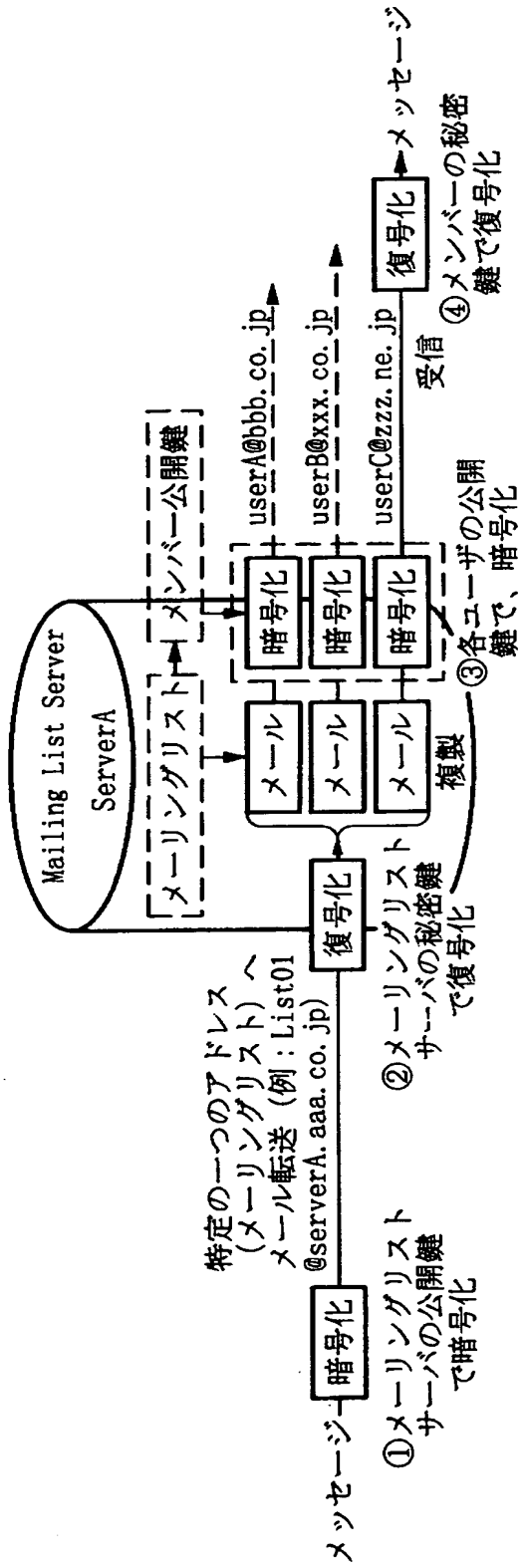
【図１２】


認証局
ネットワーク上のDB
1：メンバーリスト管理装置
チームマスター
メンバーリスト管理機能
メンバーリスト
信頼性情報の問い合わせ
(Validation、CRL)
4：メーリングリストサーバー
メッセージ
暗号化メール
user@zzz.ne.jp
受信
メンバーの秘密鍵で復号化
5
リソースデータベース
メンバーリスト
情報中継装置
メーリングリスト
暗号化メール
暗号化メール
暗号化メール
保管
保管DB
暗号化メール
情報保管サーバ
暗号化ファイル
2：暗号情報作成装置
メンバーリスト
メンバーリスト正当性確認機能
メンバーリストから公開鍵を抽出
メンバー公開鍵
特定の一つのアドレス
(メーリングリスト)へ
メール転送（例：List01
@serverA.aaa.co.jp）
複製
暗号化
メッセージ
メーリングリストサーバの公開鍵で暗号化
大きな添付ファイル
暗号化された見積書、
契約書

【図１３】


List01：userA@bbb.co.jp
userB@xxx.co.jp
userC@zzz.ne.jp
userA@bbb.co.jp
userB@xxx.co.jp
userC@zzz.ne.jp
メッセージ
受信
各受信者へ
メールを転送
Mailing List Server
ServerA
メーリングリスト
メール
メール
メール
複製
復号化
特定の一つのアドレス
（メーリングリスト）へ
メール転送（例：List01
@serverA.aaa.co.jp）
メッセージ

【図１４】


Mailing List Server
ServerA
メーリングリスト
メンバー公開鍵
暗号化
暗号化
暗号化
userA@bbb.co.jp
userB@xxx.co.jp
userC@zzz.ne.jp
メール
メール
メール
複製
③各ユーザの公開
鍵で、暗号化
受信
復号化
④メンバーの秘密
鍵で復号化
メッセージ
特定の一つのアドレス
（メーリングリスト）へ
メール転送（例：List01
@serverA.aaa.co.jp）
復号化
②メーリングリスト
サーバの秘密鍵
で復号化
暗号化
メッセージ
①メーリングリスト
サーバの公開鍵
で暗号化

【書類名】　　要約書

【要約】

【課題】　本発明の目的は、同報通信システムにおいて、サーバの管理者といえども、同報通信の通信内容を覗き見できない仕組みと、同報通信を行う受信者の脱退や、加入に対して迅速に対応でき、同報通信メンバーの動的な変更があっても、誤って同報通信してはいけないメンバーに情報を転送してしまうことのない仕組みと、サーバ管理者が同報通信の配信メンバーを管理するのではなく、同報通信を行うメンバーの中で配信メンバーを管理する仕組みと、機密情報を転送するため、多数の受信者それぞれが確実に受信できる仕組みを提供することにある。

【解決手段】　本発明の同報通信システムは、メンバーリストを管理するメンバーリスト管理装置と、暗号情報を作成する暗号情報作成装置と、暗号情報を復号化する暗号情報復号化装置と、暗号情報を中継する情報中継装置とからなる。

【選択図】　　図１

認定・付加情報

特許出願の番号	平成１０年　特許願　第３７２１８７号
受付番号	５９８００８５４２６４
書類名	特許願
担当官	髙田　良彦　　２３１９
作成日	平成１１年　２月１９日

＜認定情報・付加情報＞

【特許出願人】
- 【識別番号】 000006264
- 【住所又は居所】 東京都千代田区大手町１丁目５番１号
- 【氏名又は名称】 三菱マテリアル株式会社

【代理人】 申請人
- 【識別番号】 100064908
- 【住所又は居所】 東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
- 【氏名又は名称】 志賀　正武

【選任した代理人】
- 【識別番号】 100108578
- 【住所又は居所】 東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
- 【氏名又は名称】 髙橋　詔男

【選任した代理人】
- 【識別番号】 100089037
- 【住所又は居所】 東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
- 【氏名又は名称】 渡邊　隆

【選任した代理人】
- 【識別番号】 100101465
- 【住所又は居所】 東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
- 【氏名又は名称】 青山　正和

【選任した代理人】
- 【識別番号】 100094400
- 【住所又は居所】 東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所

次頁有

認定・付加情報（続き）

【氏名又は名称】　鈴木　三義
【選任した代理人】
【識別番号】　100106493
【住所又は居所】　東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
【氏名又は名称】　松冨　豊
【選任した代理人】
【識別番号】　100107836
【住所又は居所】　東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
【氏名又は名称】　西　和哉
【選任した代理人】
【識別番号】　100108394
【住所又は居所】　東京都台東区台東３丁目４０番１０号　村上ビル５階　高橋来山特許事務所
【氏名又は名称】　今村　健一
【選任した代理人】
【識別番号】　100108453
【住所又は居所】　東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
【氏名又は名称】　村山　靖彦

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００６２６４〕

１．変更年月日　　１９９２年　４月１０日
［変更理由］　住所変更
住　所　　東京都千代田区大手町１丁目５番１号
氏　名　　三菱マテリアル株式会社